

John M. Desmarais (SBN 320875)
DESMARAIS LLP
101 California Street
San Francisco, CA 94111
(415) 573-1900

Justin P.D. Wilcox (admitted *pro hac vice*)

jwilcox@desmaraisllp.com

Tamir Packin (SBN 317249)
110 S. 1st Street, Suite 1100

tpackin@desmaraisllp.com

Steven M. Balcof (admitted *pro hac vice*)

sbalcof@desmaraisllp.com

Carson Olsheski (admitted *pro hac vice*)

colsheski@desmaraisllp.com

David A. Frey (admitted *pro hac vice*)

dfrev@desmaraisllp.com

desmarais
DESMARAIS LLP

DESMERLEAUX
230 Park Avenue

250 Park Avenue
New York, NY 10169

212-351-3400

Attorneys for Plaintiffs

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND**

CISCO SYSTEMS, INC., a California
Corporation, CISCO TECHNOLOGY, INC., a
California Corporation

Plaintiffs,

V.

PLANTRONICS, INC., a Delaware
Corporation, WILSON CHUNG, JAMES HE,
JEDD WILLIAMS, AND THOMAS
PUORRO individuals

Defendants.

Case No.: 4:19-cv-07562-PJH

JURY TRIAL DEMANDED

SECOND AMENDED COMPLAINT FOR TRADE SECRET MISAPPROPRIATION

Plaintiffs Cisco Systems, Inc. and Cisco Technology, Inc. (collectively “Cisco”), for their Complaint against Defendants Plantronics, Inc. (“Poly”), Wilson Chung (“Dr. Chung”), James He

1 ("Mr. He"), Jedd Williams ("Mr. Williams"), and Thomas Puorro ("Mr. Puorro") hereby allege as
2 follows:

3 **Introduction**

4 1. This is an action for trade secret misappropriation by Poly and the named parties, all of
5 whom are former Cisco employees and are current or former Poly employees. Mr. Puorro, a former
6 Cisco executive and the current Executive Vice President, General Manager, Products at Poly
7 responsible for Poly's audio and video collaboration solutions, orchestrated a scheme on behalf of
8 Poly to induce Cisco employees to reveal trade secrets to him and others at Poly in an effort to unfairly
9 compete against Cisco and to "inflict pain" upon Cisco. This scheme was endorsed by Poly's most
10 senior executives, who had knowledge of, and acquiesced to, Mr. Puorro's tactics. Even after Cisco
11 brought the egregious misconduct to the attention of Poly, Poly refused to disavow the theft of Cisco's
12 trade secrets and continues to shield its employees and executives. Cisco brings this suit against Poly
13 because of Poly's continued endorsement of the scheme and its failure to take corrective action, even
14 when presented with overwhelming evidence of misconduct.

15 2. Cisco has invested significant resources to design, build, and sell its robust
16 collaboration platform, which includes unified communications and video conferencing software and
17 collaboration endpoints. Cisco's endpoint hardware includes video endpoints, telepresence units, all-
18 in-one video collaboration systems, integrated collaboration room systems, VoIP and video phones,
19 microphones, cameras, speakers, and headsets. The collaboration field is highly competitive and
20 characterized by rapid innovation. Cisco's engineers rely upon tangible and intangible financial,
21 business, scientific, technical, economic, and engineering information, such as source code,
22 schematics, design details and specifications, user feedback, design documentation, and feature
23 documentation relating to Cisco's existing and future products, as well as Cisco business information
24 such as operations, marketing, and resource strategies and plans, supplier information, cost and pricing
25 information, and payment information to develop Cisco's products. Cisco takes reasonable measures
26 to keep this information secret, and this information derives independent economic value from not
27 being generally known to, and not being readily ascertainable through proper means by, others who
28 can obtain economic value from the disclosure or use of the information.

1 3. Cisco also has made substantial and significant investments in developing its routes to
 2 market for its collaboration products and services, through extensive engagement of partner, customer,
 3 and industry connections by its global sales force. Cisco's global sales force relies upon tangible and
 4 intangible financial, business, and economic information, such as non-public financial reporting,
 5 customer lists, pricing models, forecasting, sales, resourcing, and competitive strategies and plans, and
 6 product refresh strategies to develop Cisco's go-to-market and business development plans and to
 7 market and sell Cisco products. Cisco takes reasonable measures to keep this information secret, and
 8 this information derives independent economic value from not being generally known to, and not being
 9 readily ascertainable through proper means by, others who can obtain economic value from the
 10 disclosure or use of the information.

11 4. Cisco has uncovered evidence that Dr. Chung and Mr. He, two former high-level
 12 engineers in Cisco's Unified Communications Technology Group, downloaded thousands of
 13 documents containing Cisco's highly confidential and proprietary business information ("Cisco
 14 Confidential Materials") relating to the design, manufacture, pricing, and market opportunities for
 15 both current and unreleased products. Dr. Chung undertook efforts over a period of weeks preceding
 16 his departure, and after he had accepted employment with Poly and while he was, unbeknownst to
 17 Cisco, simultaneously employed by both Cisco and Poly, to exfiltrate Cisco Confidential Materials to
 18 removable hard drives, personal email, cloud storage, and to Poly's internal intranet, and then used
 19 Cisco Confidential Materials while at Poly. When confronted with evidence of his misappropriation,
 20 Dr. Chung destroyed evidence to conceal his actions.

21 5. Mr. He joined Poly after being recruited by Dr. Chung. Prior to his departure, and after
 22 accepting his employment offer from Poly, Mr. He copied thousands of files containing Cisco
 23 Confidential Materials to an external hard drive. These documents also related to the design,
 24 manufacture, pricing, and market opportunities for both current and unreleased products. Cisco has
 25 recovered Mr. He's hard drive, and learned that Mr. He accessed a number of these documents while
 26 at Poly, and, when the misappropriation was uncovered, deleted the files to avoid detection.

27 6. Cisco also has uncovered evidence that Mr. Williams misappropriated Cisco
 28 Confidential Materials relating to Cisco's financial information and sales, business development,

1 resourcing and competitive strategies and plans, including Cisco's market data and strategies, partner
 2 margins, potential organizational restructurings, information concerning Cisco's emerging
 3 technologies, competitive focus, sales opportunities and customer lists, product pipelines, and future
 4 plans for current products. On information and belief, Mr. Williams disclosed Cisco Confidential
 5 Materials to senior executives at Poly during the recruiting and interview process and exfiltrated these
 6 materials from Cisco, including by storing an unauthorized backup of his Cisco laptop on a home
 7 server and maintaining Cisco Confidential Materials on that server after leaving Cisco and starting
 8 work at Poly. Cisco also has uncovered evidence suggesting that Mr. Williams was offered
 9 employment at Poly after proposing and disclosing to Poly Cisco Confidential Materials, including a
 10 non-public go-to-market strategy he dubbed "Project x," which had been developed and refined at
 11 Cisco and was therefore Cisco's proprietary information, and which he disclosed while employed by
 12 Cisco to both Mr. Puorro and at least two other very high ranking Poly executives.

13 7. Cisco has also uncovered evidence that Mr. Puorro, a former Cisco executive, and
 14 Executive Vice President at Poly, induced Mr. Williams to reveal Cisco's trade secrets to him and to
 15 other senior executives at Poly. As a former Cisco executive, Mr. Puorro was, or should have been,
 16 familiar with Cisco's confidentiality policies, and knew, or should have known, that the information
 17 he requested from Mr. Williams contained Cisco trade secrets and that his request for and receipt of
 18 such information interfered with Mr. Williams' obligations to Cisco.

19 8. In sum, Dr. Chung, Mr. He, Mr. Williams, and Mr. Puorro engaged in a scheme that
 20 on information and belief was endorsed by senior Poly executives and was designed to give Poly
 21 access to Cisco's trade secrets and allow Poly to unfairly compete with Cisco.

22 9. Defendants' conduct threatens to cause Cisco irreparable harm, potentially depriving
 23 Cisco of the opportunity to obtain a first-mover advantage in product development and go-to-market
 24 strategies, and depriving Cisco of business opportunities. There is also the threat that Cisco
 25 Confidential Materials will be further disclosed by Defendants, which will damage Cisco's trade secret
 26 technology and business processes.

27 10. Cisco has implemented multiple security measures to protect its trade secrets; these
 28 measures constitute reasonable measures to protect and maintain its trade secrets pursuant to 18 U.S.C.

1 §1839(3)(A). The security measures taken by Cisco include, but are not limited to, confidentiality
2 certifications and employee codes of conduct, electronic and computer-based data security, and
3 physical barriers. The following is a more detailed description of each category of Cisco's reasonable
4 trade secret protective measures:

- 5 • **Confidentiality Certifications and Employee Codes of Conduct** – Cisco's measures
6 to maintain secrecy include requirements for its employees and third-party contractors. For
7 example, Cisco employees sign Proprietary Information and Invention Assignment
8 Agreements (PIIAs), in which they agree to keep confidential Cisco's proprietary information
9 and to assign all inventions made in the course of their employment to Cisco. By way of further
10 example, Cisco employees also agree to return all company documents and materials to Cisco
11 at the end of their employment. Cisco's vendors, contractors, consultants, and partners sign a
12 Cisco Confidential Information Agreement, in which they agree, among other things, to keep
13 in confidence and trust, and not use or disclose, any Cisco trade secret to anyone outside of
14 Cisco without the prior written consent of an authorized Cisco representative. As another
15 example, Cisco employees also certify annually that they will comply with Cisco's Code of
16 Business Conduct, which prohibits, among other things, the use of Cisco assets for non-
17 company purposes. Further, Cisco conducts background checks on its employees and any
18 third-party contractors before granting them access to Cisco's data repositories. To prevent
19 the inadvertent disclosure of Cisco's trade secrets in connection with collaborations with its
20 vendors and partners, Cisco requires vendors to agree to confidentiality provisions and/or non-
21 disclosure agreements.
- 22 • **Electronic and Computer-Based Data Security** – Cisco has a Security & Trust
23 Organization tasked with managing user and administrative access to data and systems
24 (devices, applications, and services) by establishing proper controls for authentication,
25 authorization, and auditing. Cisco restricts access to certain documents on its secured
26 repositories based upon different levels of data classification to prevent disclosure, and
27 therefore, protect the secrecy of those documents. Cisco defines levels of data classifications
28 (public, confidential, highly confidential, and Cisco Restricted), which allow Cisco to

differentiate the sensitivity of data and restrict access based on the sensitivity. For access to Cisco’s internal network, Cisco requires dual-factor authentication. Cisco monitors its employees’ network activities, and maintains logs of, among other things, cloud uploads, USB downloads, and file transfers to and from Cisco’s data repositories. Cisco’s Computer Security Incident Response Team (“CSIRT”) and Data Protection and Privacy Team (“DPP”) form part of the investigative branches of the Cisco Security and Trust Organization, and provides proactive threat analysis, incident detection, and coordinated incident response by, in part, investigating incidents that involve the access and potential misuse of Cisco information by Cisco employees and vendors.

- **Physical Boundaries** – Cisco physically restricts access to its offices, network, systems, and data at least by restricting access to its facilities to only those employees or contractors with badge access.

The Parties

14 11. Plaintiff Cisco Systems, Inc., is a company duly organized and existing under the laws
15 of California, having its principal place of business at 170 West Tasman Drive, San Jose, California
16 95134.

17 12. Plaintiff Cisco Technology, Inc. is a wholly owned subsidiary of Cisco Systems, Inc.,
18 and is a company duly organized and existing under the laws of California, having its principal place
19 of business at 170 West Tasman Drive, San Jose, California 95134.

20 13. Defendant Poly is a Delaware corporation, with its principal place of business at 345
21 Encinal Street, Santa Cruz, California 95060. Poly may be served with process by serving its
22 registered agent, CT Corporation System, 818 W. Seventh Street, Ste. 930, Los Angeles, CA 90017.
23 Poly is in the IP telephony, headset, video, and collaboration space, and is a competitor to Cisco.

24 | 14. Dr. Chung is an individual residing in this jurisdiction.

25 15. Mr. He in an individual residing in this jurisdiction.

26 || 16. Mr. Williams is an individual residing outside this jurisdiction.

27 17. Mr. Puorro is an individual residing outside this jurisdiction.

Nature Of The Action

1 18. This is a civil action for violation of the Defend Trade Secrets Act (“DTSA”) under 18
 2 U.S.C. § 1836 *et seq.*, violation of Cal. Civ. Code § 3426 *et seq.*, and Intentional Interference with a
 3 Contractual Relationship.

Jurisdiction And Venue

5 19. This Court has subject matter jurisdiction over Cisco’s claims for violation of the
 6 Defend Trade Secrets Act (“DTSA”) pursuant to 28 U.S.C. §§ 1331 because they present a Federal
 7 Question.

8 20. This Court has supplemental subject matter jurisdiction of the pendent state law claims
 9 pursuant to 28 U.S.C. § 1337 because they are so related to the DTSA claims that they form part of
 10 the same case or controversy.

11 21. This Court has personal jurisdiction over Poly because its principal place of business
 12 is in this district.

13 22. This Court has personal jurisdiction over Dr. Chung because he resides in this district.

14 23. This Court has personal jurisdiction over Mr. He because he resides in this district.

15 24. This Court has personal jurisdiction over Mr. Williams at least because he has
 16 purposefully directed his activities to this forum by committing intentional acts within California
 17 causing harm to Cisco (a California corporation). Mr. Williams also purposefully directed his
 18 activities to this forum and residents thereof, by disclosing Cisco’s trade secrets to Poly and its officers,
 19 including those at Poly’s California headquarters, so that Mr. Williams could obtain a job at Poly. Mr.
 20 Williams also purposefully directed his activities to this forum through his repeated travels to
 21 California to interview with Poly, and by beginning employment with Poly in California, and by
 22 agreeing that his confidentiality obligations to Cisco shall be interpreted and enforced in accordance
 23 with the laws of the State of California. Mr. Williams also carried on a continuous course of
 24 communications with Poly’s executives in California, including communications giving rise to the
 25 claims at issue in this case. Moreover, the claims arise out of Mr. Williams’ activities within the
 26 forum. For example, as outlined in the detailed factual allegations below, Mr. Williams revealed
 27 Cisco’s trade secrets to Poly while in California, including on or around April 1, 2019, April 30, 2019,
 28

1 and June 28, 2019. Mr. Williams also created the contacts giving rise to the claims at issue in this
2 case with the forum himself, at least through his frequent and voluntary travels to Poly's headquarters
3 in California while seeking employment. Furthermore, Mr. Williams certified to Poly on October 12
4 that he did not then possess any Cisco Confidential Materials or property. Both Mr. Williams and
5 Poly knew that Mr. Williams' certification was false since, among other things, they knew Mr.
6 Williams was still employed at Cisco and Mr. Williams had access to Cisco Confidential Materials.
7 Indeed, the falsity of Mr. Williams' certification is evidenced by, among other things, the fact that he
8 uploaded Cisco Confidential Materials to a Cisco cloud storage site while he was in California after
9 executing the certification, he personally returned his Cisco laptop to Cisco in California after
10 executing the certification, and never returned the backup of his Cisco laptop that he created. The
11 false certification instigated from Poly's California office—which Poly either knew, or should have
12 known, was meaningless—evidences that neither Mr. Williams nor Poly undertook reasonable
13 protection of Cisco Confidential Materials.

14 25. This Court has personal jurisdiction over Mr. Puorro at least because Mr. Puorro
15 purposefully directed his activities to this forum, by misappropriating Cisco's trade secrets for the
16 benefit of Poly, a corporation with its principal place of business in California. In particular, Mr.
17 Puorro carried on a continuous course of direct communications with Poly's executives in California,
18 including the communications giving rise to the claims at issue in this case, such as his advocacy for
19 Mr. Williams' hiring to Poly's senior executives in California. As outlined in the detailed factual
20 allegations below, Mr. Puorro was also the guiding spirit behind Poly's wrongful conduct at issue in
21 this case. Moreover, the claim arises out of Mr. Puorro's activities within the forum. For example, as
22 outlined in the detailed factual allegations below, Messrs. Puorro and Williams were together in
23 California from April 2-5, 2019, and met in person to discuss Mr. Williams' potential employment at
24 Poly, and Cisco's collaboration product portfolio. These April meetings occurred after Mr. Williams
25 began relaying confidential details of Cisco's business to Mr. Puorro in exchange for Mr. Puorro
26 promoting Mr. Williams' employment candidacy. On information and belief, this course of conduct
27 continued during the April meetings between Messrs. Puorro and Williams in California. Moreover,

1 Mr. Puorro traveled to Santa Cruz during the week of July 1st. In that week, Mr. Puorro solicited
 2 confidential information about Cisco from Mr. Williams.

3 26. Venue is proper within this District under 28 U.S.C. § 1391(b) because a substantial
 4 part of the events or omissions giving rise to these claims occurred within this District.

5 **FACTUAL ALLEGATIONS**

6 **A. Dr. Chung**

7 27. Dr. Chung was employed at Cisco as Principal Engineer in Cisco's Unified
 8 Communications Technology Group ("UCTG"). Dr. Chung was involved in developing Cisco's
 9 collaboration products, including IP telephony solutions and audio headsets. Incumbent with this role
 10 was access to some of Cisco's most confidential trade secrets used within the UCTG, including design
 11 specifications, schematics, source code, product market analyses, and vendor contract details. On
 12 information and belief, after joining Poly, Mr. Puorro recruited Dr. Chung, and as a result of these
 13 efforts, Dr. Chung left Cisco in February 2019 to join Poly. Before doing so, Dr. Chung willfully and
 14 maliciously misappropriated Cisco Confidential Materials to use for his own benefit, and for the
 15 benefit of Poly, to the detriment of Cisco. Almost immediately after starting at Poly, Dr. Chung carried
 16 out Poly and Mr. Puorro's efforts to entice Cisco's collaboration engineers to join Poly by recruiting
 17 his former colleague, James He.

18 28. Dr. Chung began working for Cisco as a Technical Leader in March 2007.

19 29. On May 7, 2012, Dr. Chung became Principal Engineer of Cisco's UCTG.

20 30. Dr. Chung claims that his personal and Cisco laptops were stolen around Thanksgiving
 21 2018.

22 31. Subsequent to the alleged theft, Dr. Chung used a Lenovo ThinkPad X1 with serial
 23 number PF0Z3DLE ("Lenovo laptop") issued by Cisco as his primary work computer.

24 32. On November 14, 2018, Cisco also leased a MacBook Pro from IBM Global Finance
 25 which was assigned to Dr. Chung to use as a secondary work computer. Dr. Chung's department
 26 incurred the cost for this MacBook Pro. This MacBook Pro (serial number C02W186W186HV2M)
 27 ("MacBook") was shipped to Cisco and later delivered to Dr. Chung.

28 33. Dr. Chung does not own, and has never owned, the MacBook.

34. Dr. Chung is not the lessee, and has never been the lessee, of the MacBook.

35. Cisco did not authorize Dr. Chung's retention of the MacBook when his employment with Cisco ended.

36. Dr. Chung has no right to possess the MacBook after his employment with Cisco terminated, and also had no right to possess the MacBook when he began to work at Poly.

37. On February 3, 2019, Dr. Chung downloaded over 3,000 files from Cisco's internal document repositories. These documents are Cisco Confidential Materials and relate to, among other things, Cisco's contributions to 5G technology (such as its market opportunities), and design specifications of a pre-release video conferencing display prototype.

38. On February 3, 2019, Dr. Chung connected a Seagate Expansion Drive with serial number NAA77962 (“First Seagate Drive”) to his Lenovo Laptop.

39. Dr. Chung has not made the First Seagate Drive available for inspection by either Cisco or, according to Poly's General Counsel, to Poly.

40. On February 3, 2019, Dr. Chung connected a Samsung Flash Drive with serial number 374718110032913 (“Samsung Drive”) to his Lenovo laptop five times.

41. Dr. Chung copied Cisco Confidential Materials to the Samsung Drive.

42. On February 3, 2019, Dr. Chung uploaded files from the MacBook to his personal iCloud account, including Cisco's source code for debugging a user interface.

43. On February 6, 2019, Dr. Chung copied 129 files containing Cisco Confidential Materials that relate to vendor product roadmaps and a pre-release video conferencing display prototype to a Seagate Expansion SCSI Disk Device with serial number 26977AAN (“Second Seagate Drive”). The pre-release video conferencing display prototype documents included user experience design documentation, user interview feedback, artwork prototypes, and schematics.

44. On February 6, 2019, Dr. Chung connected the Samsung Drive to the Lenovo laptop four times.

45. On February 6, 2019, Dr. Chung connected a Sandisk UltraFit storage drive with serial number 4C50001291121118332 (“Sandisk Drive”) to his Lenovo laptop two times.

1 46. On information and belief, on February 6, 2019, Dr. Chung uploaded a folder entitled
2 “Toyshop” from his Lenovo laptop to cloud storage. This folder included Cisco Confidential Materials
3 such as design details and specifications relating to Cisco’s collaboration endpoints, including Cisco’s
4 sound bar products.

5 47. Dr. Chung’s misappropriation of Cisco Confidential Materials was organized,
6 premeditated, and intentional.

7 48. On February 6, 2019, Dr. Chung created various folders on the Samsung Drive named
8 after an internal Cisco project codename.

9 49. On February 6, 7, and 8, 2019, Dr. Chung created various folders on the Second Seagate
10 Drive named after numerous additional Cisco project codenames.

11 50. On February 7, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
12 laptop.

13 51. On February 8, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
14 laptop twice.

15 52. On information and belief, on February 8, 2019, Dr. Chung uploaded Cisco
16 Confidential Materials to cloud storage, including a presentation detailing go-to-market strategy,
17 design details, cost modeling, and pricing information for a pre-release video conferencing display
18 product.

19 53. On February 9, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
20 laptop twice.

21 54. On February 10, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
22 laptop.

23 55. On February 11, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
24 laptop twice.

25 56. On February 12, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
26 laptop five times.

27 57. On February 13, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
28 laptop twice.

1 58. On February 13, 2019, the MacBook was physically connected to Cisco's corporate
2 network.

3 59. On February 13, 2019, Dr. Chung informed his manager that he was leaving Cisco.

4 60. During that February 13, 2019 conversation between Dr. Chung and his manager, Dr.
5 Chung told his manager that he was not sure where he would be working, but that he was considering
6 joining Apple.

7 61. On February 14, 2019, Dr. Chung connected the Second Seagate Drive to the Lenovo
8 laptop four times.

9 62. Dr. Chung told Poly that his last day at Cisco was February 22, 2019.

10 63. Dr. Chung's last day at Cisco was, in fact, February 28, 2019.

11 64. Dr. Chung's exfiltration of Cisco Confidential Materials was outside the scope of his
12 employment at Cisco.

13 65. On February 24, 2019, Dr. Chung forwarded an email and attachment entitled "Cisco
14 UCaaS Market Position" from his Cisco email account to his personal Gmail account. The attached
15 document, clearly marked "Internal only" and "Cisco Confidential," related to Cisco's prospective
16 market positioning in the collaboration space.

17 66. On February 25, 2019, Dr. Chung downloaded more than 100 recordings of Webex
18 presentations to his Lenovo laptop. On information and belief, these recordings related to the design,
19 manufacture, pricing, and market opportunities for Cisco's Unified Communications product
20 portfolio.

21 67. On February 25, 2019, Dr. Chung connected the Second Seagate Drive to his Lenovo
22 laptop six times.

23 68. On February 25, 2019, Dr. Chung created a folder entitled "Webex_Recordings" on the
24 Second Seagate Drive.

25 69. From February 26, 2019 through February 28, 2019, Dr. Chung was an employee of
26 both Cisco and Poly.

27 70. On February 26, 2019, Dr. Chung began work at Poly.

28 71. On February 26, 2019, Dr. Chung logged into the MacBook.

1 72. On February 26, 2019, Dr. Chung emailed vendor representatives from his Cisco email
 2 account to inform them that his last day at Cisco would be February 28, 2019.

3 73. On February 26, 2019, Dr. Chung forwarded an email from his Cisco email account to
 4 his personal Gmail account. This email thread included “minutes” from a Cisco meeting.

5 74. On February 26, 2019, Dr. Chung logged into Poly’s “Sharepoint” site from the Lenovo
 6 laptop. Dr. Chung uploaded to Poly’s Sharepoint, among other things, a spreadsheet entitled
 7 Endpoints and Accessories (“EA Document”).

8 75. The EA Document contains Cisco Confidential Materials, including component
 9 specifications and competitive differentiators for Cisco’s current and not yet released hardware
 10 products.

11 76. On February 27, 2019, Dr. Chung forwarded an email from his Cisco email account to
 12 his personal Gmail account with details about a vendor contract, which also included a payment terms.

13 77. On February 27, 2019, Dr. Chung accessed his Google drive from the Lenovo laptop.

14 78. On February 27, 2019, Dr. Chung went to Cisco’s office and returned his badge and
 15 the Lenovo laptop to Cisco. Dr. Chung arrived at approximately 3:00pm, had coffee with a Cisco
 16 colleague, and posed for a group photo with members of Cisco’s UCTG. Dr. Chung did not turn in
 17 the MacBook, First Seagate Drive, Second Seagate Drive, SanDisk Drive, or Samsung Drive.

18 79. On February 28, 2019, Dr. Chung forwarded an email from his Cisco email account to
 19 his personal Gmail account with details about sensor requirements for Cisco products.

20 80. On March 8, 2019, Dr. Chung emailed the EA Document from his personal Gmail
 21 account to his Poly email account.

22 81. On March 8, 2019, Dr. Chung emailed a file marked as Cisco Confidential and entitled
 23 “Webex Workplace Vision and Strategy – Compete” (“Webex Vision Document”) from his personal
 24 Gmail account to his Poly email account.

25 82. By March 9, 2019, Dr. Chung began recruiting James He to join Poly.

26 83. As of March 28, 2019, the MacBook had not been returned to Cisco. Cisco contacted
 27 Dr. Chung to secure return of the MacBook.

1 84. On March 29, 2019, Cisco contacted Dr. Chung and requested return of the MacBook.
 2 Dr. Chung insisted that he owned the MacBook and asked Cisco to check with Cisco's IT department.

3 85. On April 9, 2019, after checking with Cisco's IT department, Cisco notified Dr. Chung
 4 that the MacBook was Cisco property and must be returned. Dr. Chung subsequently confirmed that
 5 he possessed the MacBook. Cisco followed up with Dr. Chung on April 10, April 11, April 14, April
 6 15, and April 18, but Dr. Chung refused to return the MacBook.

7 86. Dr. Chung accessed Cisco Confidential Materials while employed at Poly, including at
 8 least the EA Document, Webex Vision Document, and a Cisco collaboration roadmap document.

9 87. After being notified of Cisco's concerns that Dr. Chung had misappropriated Cisco's
 10 trade secrets, on September 26, 2019, Poly informed Cisco that it had found five documents on Dr.
 11 Chung's devices that he used at Poly, including the EA Document that Dr. Chung had previously
 12 uploaded to Poly's Sharepoint.

13 88. Dr. Chung downloaded the EA Document from Poly's Sharepoint to his new work
 14 computer issued by Poly.

15 89. On information and belief, Dr. Chung accessed this file, and other documents
 16 containing Cisco trade secret information, for his own benefit, and for the benefit of Poly, to Cisco's
 17 detriment.

18 90. On September 19, 2019, counsel for Cisco wrote Dr. Chung a letter putting Dr. Chung
 19 on notice to preserve all documents and things related to the potential misappropriation of Cisco
 20 Confidential Materials.

21 91. After receiving this preservation notice, Dr. Chung took steps to conceal his
 22 misappropriation, including destroying evidence of his unlawful conduct. For example, after receiving
 23 the preservation notice, Dr. Chung:

- 24 a. deleted iCloud backups;
- 25 b. deleted Cisco Confidential Materials from the MacBook;
- 26 c. deleted Cisco Confidential Materials from the Sandisk Drive;
- 27 d. deleted Cisco Confidential Materials from the Samsung Drive; and

1 e. propounded a demonstrably false explanation for failing to return the Second Seagate
 2 Drive to Cisco.

3 92. After receiving this preservation notice, and before delivering the MacBook, Sandisk
 4 Drive, his personal iPad, and Samsung Drive to his attorney to eventually return to Cisco, Dr. Chung
 5 performed internet searches such as “how to permanently delete icloud backup,” and “how to see what
 6 is [sic] the thumb drive without detection.”

7 93. Dr. Chung understood that his employment by Cisco created a relationship of
 8 confidence and trust with respect to confidential and proprietary information, including Cisco
 9 Confidential Materials. In order to protect Cisco Confidential Materials from use by a competitor, Dr.
 10 Chung’s Proprietary Information and Inventions Agreement (“Chung PIIA”) prohibited Dr. Chung
 11 during his employment with Cisco from becoming an employee of any other firm engaged in a
 12 business in any way competitive with Cisco or involved in the design, development, marketing, sale,
 13 or distribution of any networking or software products without first informing Cisco and obtaining its
 14 consent.

15 94. By the terms of the Chung PIIA, Dr. Chung agreed that he would “not remove any
 16 [Cisco] Documents and Materials from the business premises of [Cisco] or deliver any [Cisco]
 17 Documents and Materials to any person or entity outside of [Cisco], except as [] required to do in
 18 connection with performing the duties of [his] employment.” Dr. Chung also agreed that “immediately
 19 upon the termination of [his] employment,” he would “return all [Cisco] Documents and Materials,
 20 apparatus, equipment and other physical property, or any reproductions of such property”

21 95. Throughout its investigation into Dr. Chung’s unlawful conduct, Cisco kept Poly
 22 informed of the results of its ongoing investigation so that Poly could take necessary actions to remedy
 23 the violations. With full knowledge of Dr. Chung’s illegal activities, Poly inexplicably brought Dr.
 24 Chung back to work on November 14, 2019, leaving Cisco no choice but to file this action to protect
 25 its trade secrets. Indeed, as far back as September 9, 2019, Cisco first apprised Poly’s General Counsel
 26 of the results of Cisco’s initial investigation into Dr. Chung’s unlawful conduct. *See Exhibit A.* Cisco
 27 followed up with Poly’s General Counsel on September 19, 2019 to request a status of Poly’s review
 28

1 of the matter and further information regarding Dr. Chung's activities and employment at Poly. *See*
 2 Exhibit B.

3 96. On or about September 27, 2019, Poly's General Counsel represented to Cisco that (a)
 4 Poly had conducted an investigation into Dr. Chung's conduct, (b) Poly found that Dr. Chung had
 5 indeed brought Cisco Confidential Materials with him to Poly, and (c) Dr. Chung told Poly that he did
 6 not possess any Cisco equipment (even though he still had the MacBook Pro in his possession) and
 7 proffered a demonstrably false explanation regarding his download activities on the Second Seagate
 8 Drive and the whereabouts of the Second Seagate Drive. *See* Exhibit C. Cisco thereafter continued
 9 its investigation into Dr. Chung's activities and his purported story to Poly. On October 9, 2019, Cisco
 10 provided Poly with further details of Dr. Chung's illegal conduct, including that Dr. Chung was still
 11 employed by Cisco when he accessed Cisco's systems and sent himself Cisco Confidential Materials
 12 *while unbeknownst to Cisco* he also was employed at Poly, and requested that Poly take immediate
 13 action to protect Cisco's intellectual property exfiltrated by Dr. Chung. *See* Exhibit D.

14 97. On October 10, 2019, Poly's General Counsel confirmed that Poly had placed Dr.
 15 Chung on administrative leave. A subsequent forensic investigation by a neutral third-party of Dr.
 16 Chung's devices and cloud accounts revealed that Dr. Chung accessed additional Cisco Confidential
 17 Materials while employed at Poly, that he emailed Cisco Confidential Materials from his personal
 18 email address to his Poly email address, and that apparent data wiping procedures were performed on
 19 his devices. On the evening of November 13, after learning the alarming results of forensic
 20 investigation, Poly informed Cisco that it inexplicably intended to return Dr. Chung to his position at
 21 Poly the next day, precipitating the filing of the original Complaint on November 18, 2019.

22 98. The trade secrets misappropriated by Dr. Chung have independent economic value.

23 99. First, Cisco has invested significant resources in the creation of these particular trade
 24 secrets:

- 25 • **Design specifications and schematics for Cisco's pre-release video conferencing**
 26 **prototype** – These specifications are the end result of Cisco's carefully orchestrated and labor-
 27 intensive design process. The pre-release video conferencing prototype is complex: it requires
 28 a completed industrial design, an advanced processor system to coordinate and synchronize

1 the functions of other hardware components, a printed circuit board for electrically connecting
2 various components, video components, acoustic components, and an advanced thermal
3 design. The design process of these products is iterative. For example, a change to the thermal
4 design requires corresponding changes to dependent components such as acoustic and video
5 systems, as well as changes to the printed circuit board. As another example, if a designer
6 chooses a particular set of speakers for use in the endpoint, that decision will constrain the
7 industrial design, because acoustic performance depends on various geometric parameters,
8 such as volume, reverberation, and sound absorption. Accordingly, the component selection
9 and layout, which is reflected in Cisco's design specifications for the pre-release video
10 conferencing prototype, must be carefully orchestrated in the design process. These
11 development efforts require the coordinated efforts of a team of engineers for many months.
12 The end result of the design process includes design specifications, which allow production of
13 the system at scale without requiring the manufacturer to repeat Cisco's iterative design
14 process. Thus, design specifications and schematics for Cisco's pre-release video conferencing
15 prototype are valuable at least because they allow Cisco to manufacture these products for
16 resale at scale at a competitive cost. Cisco's financial investment in these design specifications
17 and schematics for Cisco's pre-release video conferencing prototype includes engineers'
18 compensation, raw materials, off-the-shelf components, and third-party vendors, among other
19 things.

- 20 • **Design details and specifications for Cisco's sound bar products** – Cisco's sound
21 bar products follow the iterative process outlined above for Cisco's video conferencing
22 prototype, except that stand-alone sound bar products do not include an integrated video
23 component. Thus, design details and specifications for Cisco's sound bar products are valuable
24 at least because they allow Cisco to manufacture these products for resale at scale at a
25 competitive cost. Cisco's financial investment in these design details and specifications for
26 Cisco's sound bar products also includes engineers' compensation, raw materials, off-the-shelf
27 components, and third-party vendors, among other things.

- 1 • **Artwork prototypes, user experience design documentation, and user interview**
2 **feedback** – This information reflects Cisco’s investment in the user experience, and the
3 coordinated efforts of its product design team and user experience professionals. In particular,
4 Cisco evaluates consumer preferences when designing a product, which informs what the
5 product will look like, what features will be offered, and how much it costs. The results of this
6 research are Cisco’s artwork prototypes and user feedback, which are used by Cisco’s design
7 teams in the iterative design process. Thus, artwork prototypes, user experience design
8 documentation, and user interview feedback are valuable to Cisco at least because they provide
9 consumer insights, thus allowing Cisco to meet market demands in its commercial products.
10 Cisco’s financial investment in these artwork prototypes, user experience design
11 documentation, and user interview feedback includes engineers’ compensation, and third-party
12 vendors, among other things.
- 13 • **Source code** – The misappropriated source code reflects engineer development time,
14 which includes but is not limited to problem identification, solution conception, flow charting,
15 pseudo-code authorship, code authorship, testing and debugging, and quality assurance. In
16 addition to its engineers’ development efforts, Cisco’s source code also reflects the collective
17 expertise of its engineers and product development teams. Cisco’s financial investment in this
18 source code includes software engineers’ compensation, and third-party vendors, among other
19 things.
- 20 • **The EA Document** – The EA document misappropriated by Dr. Chung identifies more
21 than two dozen Cisco collaboration products by code name. For each product, it identifies
22 critical component selection choices made by Cisco’s design team in the course of product
23 development, and reflects thousands of hours of engineers’ labor in making these decisions.
24 As an example, Cisco’s engineers devote considerable time to evaluating various CPU
25 components for its collaboration products, including those that have not been commercially
26 released, and makes these investments to determine which chips provide the optimal
27 combination of cost and performance. The EA document summarizes the end-result of Cisco’s
28 engineering efforts, and thus is valuable to Cisco at least because it summarizes the competitive

1 differentiators and product development plans, which, if known to competitors, would provide
2 insights into Cisco's product development roadmap and deprive Cisco of a first-mover
3 advantage. Cisco's financial investment in the information summarized in the EA Document
4 includes engineer's compensation, raw materials, off-the-shelf components, and third-party
5 vendors, among other things.

6 100. Second, Cisco took precautions to protect the secrecy of the trade secrets stolen by Dr.
7 Chung. Dr. Chung's PIIA required him to keep the materials he misappropriated secret. In particular,
8 it required that he protect "Proprietary Information," which includes trade secrets, source code,
9 designs, product development plans, and research and development. Each of the trade secrets Dr.
10 Chung misappropriated constitutes Proprietary Information under Dr. Chung's PIIA. Thus, Dr. Chung
11 understood and agreed that his employment created a relationship of confidence and trust with respect
12 to the information he misappropriated. Additionally, pursuant to his PIIA, Dr. Chung was prohibited
13 from removing Proprietary Information from the business premises of Cisco or delivering it to any
14 person or entity outside of Cisco, except as required in connection with performing the duties of his
15 employment. Also, by signing the PIIA, Dr. Chung agreed that immediately upon the termination of
16 his employment, he would return all Proprietary Information to Cisco. Cisco also protected the
17 Proprietary Information that Dr. Chung could access as a high-ranking Cisco engineer, including the
18 trade secrets at issue in this case, by requiring that he annually certify that he would not use Cisco
19 assets for non-company purposes. Cisco also protected the trade secrets at issue here with electronic
20 and computer-based data security. For example, Cisco monitored Dr. Chung's network activity, and
21 thus was able to identify the time, date, and file name of the documents that he copied from Cisco's
22 network to his personal storage drives. With those electronic and computer-based data security
23 precautions, Cisco was able to ascertain the date, manner, scope, and other details pertaining to Dr.
24 Chung's exfiltration of thousands of Cisco documents. Those details are reflected in the factual
25 allegations in this pleading. Cisco also restricts access to its offices and data systems to current
26 employees, a precaution that Dr. Chung overcame through deception, by failing to inform Cisco that
27 he became a Poly employee on February 26, 2019 while still employed by Cisco.

28

1 101. Third, others were willing to pay for access to the trade secrets stolen by Dr. Chung.
 2 In particular, Dr. Chung used the trade secrets in the course and scope of his employment at Poly, for
 3 which he was paid a salary. As one example, with respect to the EA Document, Dr. Chung emailed
 4 that document to his Poly business email address and uploaded it to Poly's internal "Sharepoint"
 5 document sharing site. As another example, Dr. Chung has retained and refuses to return the Second
 6 Seagate Drive, which, on information and belief, presently contains design specifications and
 7 schematics for Cisco's pre-release video conferencing prototype, design details and specifications for
 8 Cisco's sound bar products, Cisco's artwork prototypes, Cisco's user experience design
 9 documentation, Cisco's user interview feedback, and Cisco's source code. On information and belief,
 10 Dr. Chung refuses to return these materials, at least in part because he uses them in the course and
 11 scope of his employment at Poly.

12 102. Fourth, in addition to Cisco's development efforts, the trade secrets stolen by Dr.
 13 Chung also reflect the collective expertise of Cisco's engineers and product development teams. If
 14 these trade secrets were to become public, competitors could exploit them to shorten their own
 15 development timelines, by using them to guide internal development efforts or to outright copy Cisco's
 16 proprietary designs. For example, Poly designs and manufactures collaboration devices such as sound
 17 bars, headsets, telephones, and video endpoints and could use Cisco's design specifications as
 18 development shortcuts. In addition, even if Poly did not copy or mimic Cisco's design specifications,
 19 knowledge of Cisco's designs, product development strategies, and roadmaps, particularly when they
 20 pertain to unreleased products, enables Poly to tailor its own solutions to anticipate Cisco's product
 21 roadmap before that information is publicly available. That advance notice gives Poly an economic
 22 advantage and deprives Cisco of a first-mover advantage.

23 **B. Mr. He**

24 103. Mr. He was an engineer with Cisco, who played an integral role in developing many of
 25 Cisco's successful products. Incumbent with Mr. He's responsibilities was access to some of Cisco's
 26 most confidential trade secrets used within Cisco's UCTG, including design specifications,
 27

28

1 schematics, source code, product market analyses, and vendor contract details. Mr. He left Cisco in
 2 June 2019 to join Poly.

3 104. Before leaving Cisco, Mr. He, without authorization, willfully and maliciously
 4 misappropriated Cisco's confidential and proprietary business information to use for his own benefit,
 5 and for the benefit of Poly, to the detriment of Cisco.

6 105. On March 1, 2019, Dr. Chung communicated details of his new position at Poly to Mr.
 7 He.

8 106. On March 9, 2019, Dr. Chung told Mr. He that Poly was interested in having Mr. He
 9 work there.

10 107. Mr. He regularly took photographs of Cisco Confidential Materials on his iPhone Max.

11 108. For example, on May 13, 2019, Mr. He took a photograph of a financial presentation
 12 containing Cisco Confidential Materials, which included Cisco's Q3 financial highlights, largest deals,
 13 and comparative revenue by category.

14 109. On May 30, 2019, Mr. He copied Cisco Confidential Materials, including architectural
 15 design documents relating to Cisco's unreleased headset concepts to a LaCie external hard drive with
 16 serial number 0000NL37HDBX ("LaCie Drive").

17 110. On June 1, 2019, Mr. He traveled from his home in China to California. Mr. He told
 18 his manager that this was a personal trip. Mr. He remained in California until June 9, 2019.

19 111. On June 3, 2019, Mr. He took a photo from his iPhone Max of a hardware diagram for
 20 a Cisco headset prototype.

21 112. On June 5, 2019, Mr. He took photographs from his iPhone Max of Cisco Confidential
 22 Materials that discussed Cisco's emerging business opportunities in the collaboration space. On this
 23 date, Mr. He also downloaded a headset test report containing Cisco Confidential Materials.

24 113. On June 6, 2019, Mr. He informed his manager that he was resigning from Cisco.

25 114. On June 6, 2019, Mr. He connected to Cisco's Virtual Private Network from a Comcast
 26 IP address in the United States.

27 115. While on Cisco's VPN in the United States on June 6, 2019, Mr. He copied over 100
 28 documents to the LaCie Drive. These documents included Cisco Confidential Materials, such as

1 design and configuration documents relating to Cisco's unreleased headset prototypes. Also included
2 in these files was information relating to vendor roadmaps for Cisco's products.

3 116. On June 10, 2019, Mr. He had an in-person meeting with his manager in China. In this
4 meeting, Mr. He discussed his resignation with his manager. Mr. He stated that he was not going to
5 Poly, but that he was moving to Guangzhou for family reasons.

6 117. On June 11, 2019, Mr. He copied an email archive from his Cisco email account to the
7 LaCie Drive. On June 14, 2019, Mr. He copied two additional archives from his Cisco email account
8 to the LaCie Drive. These archives contain Cisco Confidential Materials. Discussions over email
9 contained in the archive reflect Cisco's strategic product development decisions. The email archives
10 also include, as email attachments, technical design documents and presentations containing Cisco's
11 trade secrets.

12 118. On June 17, 2019, Mr. He copied approximately 200 emails from his Cisco email trash
13 folder to the LaCie Drive. These emails contain Cisco Confidential Materials and relate to design
14 details for a then unreleased IP telephone project.

15 119. On June 18, 2019, Mr. He copied approximately 1500 files to the LaCie Drive. These
16 files contain Cisco Confidential Materials and include internal emails, architectural documents,
17 marketing plans, and cost information.

18 120. On June 20, 2019, Mr. He copied approximately 90 files to the LaCie Drive. These
19 files contain Cisco Confidential Materials and relate to Cisco's headset projects.

20 121. On June 21, 2019, Mr. He left Cisco. Mr. He retained the LaCie Drive.

21 122. Mr. He's exfiltration of Cisco Confidential Materials was outside the scope of his
22 employment at Cisco.

23 123. On information and belief, Mr. He joined Poly on or around June 24, 2019.

24 124. On June 27, 2019, Mr. He accessed Cisco Confidential Materials stored on the LaCie
25 Drive, including a schematic for an unreleased IP telephone project. Mr. He again accessed this file
26 on July 3, 2019.

27 125. On July 1, 2019, Mr. He accessed Cisco Confidential Materials stored on the LaCie
28 Drive, including a vendor's roadmap update created for Cisco.

1 126. On July 15, 2019, Mr. He accessed Cisco Confidential Materials stored on the LaCie
 2 Drive, including a full engineering specification for a next-generation conference room collaboration
 3 device. Mr. He had previously copied this file to the LaCie Drive on May 30, 2019.

4 127. On information and belief, Mr. He accessed these Cisco Confidential Materials for his
 5 own benefit, and for the benefit of Poly, to Cisco's detriment.

6 128. On August 2, 2019, counsel for Cisco put Mr. He on notice to preserve all documents
 7 and things related to the potential misappropriation of Cisco's confidential and proprietary business
 8 information.

9 129. On August 5, 2019, after receiving the preservation notice, Mr. He took steps to conceal
 10 his misappropriation, including destroying evidence of his unlawful conduct. By way of example, on
 11 August 5, Mr. He deleted thousands of Cisco files containing Cisco Confidential Materials from the
 12 LaCie Drive. On information and belief, Mr. He deleted these files because Poly had commenced an
 13 internal investigation into the misappropriation, and Mr. He was requested to turn the LaCie Drive to
 14 Poly's investigators. In addition to the aforementioned files and file types, Mr. He deleted various
 15 source code library stacks from the LaCie Drive.

16 130. On August 2, 2019, Cisco notified Poly that Mr. He had misappropriated Cisco
 17 Confidential Materials. Poly investigated Cisco's allegations and terminated Mr. He's employment
 18 with Poly shortly thereafter.

19 131. Mr. He understood that his employment by Cisco created a relationship of confidence
 20 and trust with respect to confidential and proprietary information.

21 132. By the terms of Mr. He's Proprietary Information and Inventions Agreement ("He
 22 PIIA"), Mr. He agreed that he would "not remove any [Cisco] Documents and Materials from the
 23 business premises of [Cisco] or deliver any [Cisco] Documents and Materials to any person or entity
 24 outside [Cisco], except as [] required to do in connection with performing the duties of [his]
 25 employment." Mr. He also agreed that "immediately upon the termination of [his] employment," he
 26 would "return all [Cisco] Documents and Materials, apparatus, equipment and other physical property,
 27 or any reproductions of such property"

28 133. The trade secrets misappropriated by Mr. He have independent economic value.

1 134. First, Cisco has invested significant resources in the creation of these particular trade
 2 secrets:

3 • **Architectural design documents and hardware diagrams for headset prototypes** –

4 These specifications are the end result of Cisco's orchestrated and labor-intensive design
 5 process. The headset prototype is complex: its design requires a completed industrial design,
 6 audio processing equipment, microphone, speakers, System on a Chip (SOC), and a printed
 7 circuit board (PCB). Additionally, it required advanced acoustic design, including, for
 8 example, acoustic echo cancellation and the effects of foam pad variation on RMS. Changes
 9 to particular components also necessitate alterations to other, dependent components. For
 10 example, component modifications may require alterations to the products industrial design.
 11 As another example, if a designer chooses a particular set of speakers for use in the headset,
 12 that decision will constrain the industrial design, because acoustic performance depends on
 13 various geometric parameters, such as volume, reverberation, and sound absorption.
 14 Accordingly, the component selection and layout, which are reflected in Cisco's design
 15 specifications for its headset prototypes, must be carefully orchestrated in the design process.
 16 These development efforts require the coordinated efforts of a team of engineers for many
 17 months. The end result of the design process are design specifications, including architectural
 18 design documents and hardware diagrams, which allow production of the system at scale
 19 without requiring the manufacturer to repeat Cisco's iterative design process. Thus,
 20 architectural design documents and hardware diagrams for headset prototypes are valuable at
 21 least because they allow Cisco to manufacture these products for resale at scale at a competitive
 22 cost. Cisco's financial investment in these Architectural design documents and hardware
 23 diagrams for headset prototypes includes engineers' compensation, raw materials, off-the-shelf
 24 components, and third-party vendors, among other things.

25 • **Design details and schematics for unreleased IP telephone project** – As with
 26 Cisco's headset prototypes, Cisco invests heavily in its IP telephone projects, even including
 27 those that do not become commercially available. As with commercially available products,
 28 Cisco's unreleased products require thousands of hours of engineering time, raw materials,

1 shelf components, and third-party vendors, among other things. In addition to being valuable
 2 as potential future products, unreleased products reflect negative know-how, and inform
 3 Cisco's future design decisions on what not to do. Thus, design details and schematics for the
 4 unreleased IP telephone project are valuable at least because they embody know-how that is
 5 part of the corpus of engineering knowledge that Cisco uses to develop its cutting-edge
 6 collaboration product portfolio.

7 • **Cisco's emerging business opportunities in the collaboration space** – In addition to
 8 investing in product development, Cisco also invests in market research to identify sales and
 9 partnership opportunities as a way to introduce its products into the marketplace. Through
 10 direct customer engagement, Cisco's sales and marketing teams identify existing deals and
 11 deal pipelines to focus the efforts of its sales representatives. Cisco builds long-term
 12 relationships with its customers and its partners. These coveted relationships result in long
 13 term deals and deal pipelines, which Cisco values both as a source of revenue and as a means
 14 to predict revenue and identify roadblocks in the sales process. Information about these
 15 emerging business opportunities in the collaboration space is valuable to Cisco at least because
 16 it identifies customers and targeted deals, allowing Cisco's sales force to target previously
 17 identified commercial opportunities to maximize efficiencies. Cisco's financial investment in
 18 these emerging business opportunities in the collaboration space includes sales and marketing
 19 compensation, travel, product demos, customer support, office space, and third-party vendors,
 20 among other things.

21 • **Vendor product roadmaps** – Cisco's investments in its vendors, including its
 22 significant buying power and substantial purchase history, encourage vendors to keep Cisco
 23 apprised of their own product development efforts in order to promote future sales. Because
 24 of Cisco's buying power and substantial purchase history, vendors tailor their offerings to
 25 Cisco's needs, and provide information about their own product pipelines before that
 26 information becomes publicly available. Cisco values this information because it facilitates
 27 product development planning. For example, if Cisco knows when a vendor will have a SoC
 28 with particular capabilities commercially available, Cisco can plan its own product roadmap

1 accordingly. Cisco's financial investment in these vendor product roadmaps includes its
 2 extensive purchasing history with these vendors, among other things.

- 3 • **Full engineering specifications** – When a product design is complete, the design
 4 parameters are embodied in engineering specifications. Full engineering specifications reflect
 5 the materials that Cisco sends to its manufacturing partners to enable them to physically make
 6 the products without duplicating Cisco's iterative design process. These specifications are the
 7 end result of Cisco's design process, and access to full specifications would enable a
 8 competitor simply to bypass product design, or the efforts involved in reverse engineering, and
 9 take Cisco's specifications to a contract manufacturer. Thus, full engineering specifications
 10 are valuable to Cisco at least because they allow Cisco to manufacture products for resale at
 11 scale at a competitive cost. Accordingly, Cisco's financial investment in these full engineering
 12 specifications includes engineers' compensation, raw materials, off-the-shelf components, and
 13 third-party vendors, among other things.

14 135. Second, Cisco took precautions to protect the secrecy of the trade secrets stolen by Mr.
 15 He. Mr. He's PIIA required him to keep the materials he misappropriated secret. In particular, it
 16 required that he protect "Proprietary Information," which includes secrets, source code, designs,
 17 business development plans, product development plans, research, and development. Each of the trade
 18 secrets Mr. He misappropriated constitutes Proprietary Information under Mr. He's PIIA. Thus, Mr.
 19 He understood and agreed that his employment created a relationship of confidence and trust with
 20 respect to the information he misappropriated. Additionally, pursuant to his PIIA, Mr. He was
 21 prohibited from removing Proprietary Information from the business premises of Cisco or delivering
 22 it to any person or entity outside of Cisco, except as required to do in connection with performing the
 23 duties of his employment. Also, by signing the PIIA, Mr. He agreed that immediately upon the
 24 termination of his employment, he would return all Proprietary Information to Cisco. Cisco also
 25 protected the Proprietary Information that Mr. He could access as a high-ranking Cisco engineer,
 26 including the trade secrets at issue in this case, by requiring that he annually certify that he would not
 27 use Cisco assets for non-company purposes. Cisco also protected the trade secrets at issue here with
 28 electronic and computer-based data security. For example, Cisco monitored Mr. He's network

1 activity, and thus was able to identify the time, date, and file name of the documents that he copied
 2 from Cisco's network to his personal storage drives. With those electronic and computer-based data
 3 security precautions, Cisco was able to ascertain the date, manner, scope, and other details pertaining
 4 to Mr. He's exfiltration of thousands of Cisco documents. Those details are reflected in the factual
 5 allegations in this pleading. Cisco also restricts access to its offices and data systems to current
 6 employees.

7 136. Third, others were willing to pay for access to the trade secrets stolen by Mr. He. In
 8 particular, Mr. He used the trade secrets in the course and scope of his employment at Poly, for which
 9 he was paid a salary. For example, while employed and paid by Poly, Mr. He accessed at least the
 10 schematic for an unreleased IP telephone project, the vendor roadmap update, and the full engineering
 11 specification for a next-generation conference room device.

12 137. Fourth, in addition to Cisco's development efforts, the trade secrets stolen by Mr. He
 13 also reflect the collective expertise of Cisco's engineers and product development teams. If these trade
 14 secrets were to become public, competitors could exploit them to shorten their own development
 15 timelines, by using them to guide internal development efforts or to outright copy Cisco's proprietary
 16 designs. For example, Poly designs and manufactures collaboration devices such as sound bars,
 17 headsets, telephones, and video endpoints and could use Cisco's design specifications as development
 18 shortcuts. In addition, even if Poly did not copy or mimic Cisco's design specifications, knowledge
 19 of Cisco's designs, Cisco's product development strategies, and Cisco's roadmaps, particularly when
 20 they pertain to unreleased products, enables Poly to tailor its own solutions to anticipate Cisco's
 21 product roadmap before that information is publicly available. That advance notice gives Poly an
 22 economic advantage and deprives Cisco of a first-mover advantage.

23 **C. Messrs. Williams & Puorro**

24 138. Mr. Williams was a Regional Sales Director in ASP Architectures when he terminated
 25 his employment at Cisco in October 2019. Prior to that, he was a Director in Global Collaboration
 26 Sales, in which he had global responsibility for developing sales and marketing strategies for bringing
 27 Cisco's suite of collaboration products to market. Mr. Williams started at Cisco in 1998 as a Systems
 28 Engineer II.

139. Mr. Puorro is the Executive Vice President and General Manager of Products at Poly. On information and belief, Mr. Puorro is the Poly executive officer chiefly responsible for its product development efforts. Mr. Puorro was a Cisco employee from October 2009 until December 2018. Mr. Puorro served as Vice President of Cisco's Unified Communications Technology Group from October 2014 until December 2018. Mr. Puorro left Cisco in December 2018, and, on information and belief, Mr. Puorro joined Poly in January 2019.

140. Mr. Williams stored his iPhone messages in his iCloud account. While employed at Cisco, Mr. Williams synced his iPhone messages from iCloud account to his Cisco laptop, which saved a local copy of his iPhone messages on his Cisco laptop.

141. Beginning in February 2019, Mr. Williams began aggressively pursuing employment with Poly. Mr. Williams sought out and received the assistance of Mr. Puorro and other third-parties to advocate for his candidacy at Poly. Mr. Puorro initiated a scheme whereby he would exchange coaching and advocacy on Mr. Williams' behalf for confidential details about Cisco's competitive business. As part of this scheme, Mr. Williams shared with Mr. Puorro and other Poly executives information about upcoming organizational restructurings at Cisco before they were announced to enable Poly's recruitment of Cisco employees identified by Mr. Williams and Mr. Puorro, essentially acting as an agent for Poly within Cisco and while being employed and compensated by Cisco.

9/11/2019 3:01:17 PM; Mr. Williams: I'm a huge [Cisco Employee] fan - I've seen him work miracles over the last 15 years. [REDACTED] - that guy is a sales machine

9/11/2019 3:04:03 PM; Poly Executive: Been talking to [Consultant]?

9/11/2019 3:05:20 PM; Mr. Williams: No - but I gave [Cisco Employee] the heads-up about 30 days ago that there was an external job that may be opening up that he should consider if he gets a call. He connected the dots.

9/11/2019 3:06:28 PM; Poly Executive: Got it

* * *

9/12/2019 2:14:12 PM; Mr. Williams: We are going to execute another LR in two weeks

9/12/2019 6:09:57 PM: Mr. Puorro: Nice

9/12/2019 6:10:12 PM; Mr. Williams: [Cisco Employee] and I had another conversation

9/12/2019 6:10:55 PM; Mr. Williams: if you want him - I think you can get him - but it can't be like me - you have to do it quickly. He's got two very real other jobs he's looking at

1 142. As Mr. Williams grew more desperate for employment with Poly, Mr. Williams shared
2 with Mr. Puorro and other third parties increasingly sensitive Cisco Confidential Materials. For
3 example, in preparation for an interview with Poly, Mr. Williams shared highly confidential and non-
4 public financial information relating to bookings for Cisco's collaboration business with a third-party
5 consultant who, at the time, Mr. Puorro was trying to bring into Poly, and who shortly thereafter began
6 work at Poly. Further still, Mr. Williams eventually revealed details of various Cisco sales and
7 marketing strategies to Poly's highest ranking executives in order to secure employment. In so doing,
8 Mr. Puorro solicited, and Mr. Williams willfully and maliciously shared, Cisco's trade secrets to
9 "inflict pain" upon Cisco. For example, Mr. Williams, while preparing for an interview with Poly,
10 shared a detailed presentation outline that Mr. Williams' intended to deliver to Poly with the third-
11 party consultant, who would later become employed by Poly himself, containing Cisco's sensitive and
12 non-public financial information. On information and belief, Mr. Williams shared this information
13 with Poly's highest ranking executives while interviewing with Poly. Excerpts from this document
14 are seen below:

15
16
17
18
19
20
21
22
23
24
25
26
27
28

1

2 Good morning!

3

I'm remain super excited about the opportunity to come work for you [REDACTED]

4

How are things going for you?

5

How's the sales meeting?

6

Based upon our last conversation I thought I'd share with you a couple of additional items:

7

1. The Mix of our business across Public Sector, Enterprise, Commercial.
2. How I drive the RTM each and every day with though our channel partners:

8

a) Working with Channels at Cisco [REDACTED]

9

[REDACTED] Everything we do [REDACTED]

10

I may not have emphasized this during our conversations, and that may be due to
the fact that [REDACTED]

11

3. Some aggressive thoughts on how to take advantage of the market transition and
opportunity happening now.
4. References for Jedd

12

13

The Mix of the Business:

14

I thought it would be good to share with you the mix of my business and where I spend the
majority of my time when it comes to Collaboration.

15

Globally: [REDACTED]

16

- [REDACTED]
- [REDACTED]
- [REDACTED]

17

Americas: [REDACTED] in revenue broke down across these segments/countries:

18

- [REDACTED]

19

20

21

22

143. Collectively, Mr. Williams, Mr. Puorro, and other senior Poly executives knew that
their conduct was unlawful. Indeed, they took steps to conceal their illegal conduct by communicating
through their personal email addresses (and not their Poly email, which on information and belief, they
use for Poly business) and reverting to live discussions so that the details of their communications
would not be discovered, because they did not, in their words, "want to put anything on [t]ext that
[they] don't want Cisco to have."

28

1 144. In February 2019, shortly after Mr. Puorro left Cisco for Poly, Mr. Williams contacted
 2 Mr. Puorro to ask about employment opportunities at Poly. Mr. Williams was eager to move on from
 3 Cisco, and sought out Mr. Puorro’s assistance with the job search.

4 145. Mr. Puorro advocated for Mr. Williams’ candidacy at Poly. For example, as soon as
 5 Mr. Williams expressed interest in joining Poly, Mr. Puorro spoke favorably of Mr. Williams to a Poly
 6 sales executive (“First Poly Executive”). Mr. Puorro’s advocacy was effective—the First Poly
 7 Executive reached out to Mr. Williams days later and arranged for an in-person interview. Mr. Puorro
 8 also secured expedited consideration for Mr. Williams. For example, when he learned that Mr.
 9 Williams’ interview with the sales executive would not occur until the following week, Mr. Puorro
 10 arranged for a high ranking Poly executive (“Second Poly Executive”) to contact Mr. Williams
 11 personally the next day.

12 146. On March 3-4, 2019, Mr. Williams interviewed with executives at Poly. After the
 13 interviews, Mr. Williams immediately reached out to Mr. Puorro to discuss the interviews. Mr.
 14 Williams indicated that his total target compensation threw the First Poly Executive “a curve ball” and
 15 that Mr. Williams received a “let’s stay in touch” message. As he would throughout Mr. Williams’
 16 interview process, Mr. Puorro counseled Mr. Williams on how to navigate these interviews and
 17 interact with Poly’s executives. For example, Mr. Puorro communicated to Mr. Williams that
 18 compensation is just a decision point, and that he should follow up with the Second Poly Executive in
 19 a couple of days. Mr. Puorro maintained regular contact and ensured that Mr. Williams was following
 20 his guidance.

21 147. On information and belief, Mr. Puorro provided guidance to Mr. Williams and
 22 advocacy for his candidacy within Poly to secure Mr. Williams as a source within Cisco for Cisco
 23 Confidential Materials. Mr. Puorro regularly requested confidential details of Cisco’s business from
 24 Mr. Williams. These requests escalated in sensitivity, and frequently coincided with times when Mr.
 25 Puorro’s advocacy would be most beneficial to Mr. Williams. On information and belief, Mr. Puorro
 26 traded upon Mr. Williams’ desperation for a senior position at Poly and his own apparent ability to
 27 expedite consideration to induce Mr. Williams to reveal Cisco’s trade secrets. Early on in the
 28 recruitment process, Mr. Puorro tested Mr. Williams’ willingness to reveal sensitive information.

1 148. On March 6, 2019, while Mr. Williams was in San Diego, California, Mr. Puorro asked
 2 Mr. Williams if “org changes” had happened at Cisco. Mr. Williams provided a detailed response.
 3 After Mr. Williams provided these details, he explained that he was ready to move on from Cisco.
 4 Mr. Puorro reassured him that the Second Poly Executive would promptly respond to Mr. Williams’
 5 requests for employment.

6 149. Mr. Puorro would use Poly’s protracted recruitment procedures to his advantage in
 7 inducing Mr. Williams to reveal Cisco Confidential Materials. On information and belief, Mr. Puorro
 8 would present delays as opportunities to advocate on Mr. Williams’ behalf, with the understanding
 9 that Mr. Williams would provide sensitive details about Cisco’s business in return.

10 150. For example, on March 7, 2019, Mr. Puorro informed Mr. Williams that another
 11 individual already had the position Mr. Williams was seeking at Poly. Mr. Puorro asked Mr. Williams
 12 for some time to work with the Second Poly Executive to bring Mr. Williams to Poly.

13 151. Apparently in response, and desperate to prove his usefulness to Poly, on the following
 14 day, March 8, 2019, Mr. Williams provided information to Mr. Puorro about organizational changes
 15 at Cisco. Mr. Puorro requested further details, and on information and belief, Mr. Williams provided
 16 such details.

17 152. On March 13, 2019, less than a week after Mr. Puorro told Mr. Williams that he would
 18 work to bring him into Poly and knowing that Mr. Puorro was interested in learning about
 19 “organization changes” at Cisco before they were made public, Mr. Williams communicated to Mr.
 20 Puorro that he had access to, and was willing to share, the names of individuals who would be impacted
 21 by upcoming organizational changes and encouraged Mr. Puorro that now was the time to act to disrupt
 22 Cisco (dubbed “Project x”):

23 3/11/2019 2:35:32 PM; Mr. Puorro: talk?

24 3/11/2019 2:36:12 PM; Mr. Williams: Yes sir

25 3/13/2019 5:35:31 PM; Mr. Williams: Time is now to recruit. Let’s execute a project x like we did
 26 with [another company.]

27 3/13/2019 5:35:42 PM; Mr. Williams: I have a list

28 153. On March 18, 2019, Mr. Puorro informed Mr. Williams that he had spoken to the
 Second Poly Executive about Mr. Williams, and Mr. Puorro asked to meet with Mr. Williams. Mr.

1 Puorro and Mr. Williams met in person the next day to discuss Mr. Williams' potential employment
 2 at Poly.

3 154. On March 22, 2019, Mr. Williams communicated highly confidential details about a
 4 matter at Cisco, including Cisco's legal strategy, to Mr. Puorro.

5 155. Mr. Puorro, in addition to advocating for Mr. Williams' candidacy, counseling him on
 6 how to interact with Poly's other senior executives, and sharing how his candidacy was being
 7 perceived at Poly, also conveyed his own importance in the recruitment process to Mr. Williams. For
 8 example, Mr. Puorro communicated that it was he and the Second Poly Executive who would get Mr.
 9 Williams to Poly, and Mr. Puorro made key introductions for Mr. Williams.

10 156. On April 1, 2019, Mr. Puorro traveled to California for Poly business. On April 2,
 11 2019, Mr. Williams traveled to San Jose, California to meet with Mr. Puorro and other Poly employees
 12 to further discuss Mr. Williams' potential employment at Poly and, on information and belief, Cisco's
 13 collaboration business. Both Mr. Williams and Mr. Puorro stayed in California until April 5, 2019.

14 157. On information and belief, Mr. Puorro offered his assistance in exchange for Mr.
 15 Williams revealing increasingly sensitive Cisco Confidential Materials. When Mr. Williams did not
 16 offer these materials, Mr. Puorro's advice was terse, insubstantial, or non-existent.

17 158. On April 30, 2019, Mr. Williams was in Santa Cruz, California for interviews with Poly
 18 senior executives.

19 159. On May 9, 2019, Mr. Williams relayed details from Cisco's Global Collaboration
 20 Quarterly Business Review meeting to Mr. Puorro, and suggested that he could provide information
 21 about Cisco in exchange for an offer with Poly:

22 5/9/2019 6:36:00 PM; Mr. Williams: [Cisco Employee] telling everyone you are now the guy at Poly

23 5/9/2019 6:36:09 PM; Mr. Williams: He covered it off at the Global Collab QBR

24 5/9/2019 7:21:47 PM; Mr. Puorro: We need to find out how [Cisco Employee] knew that.

25 5/9/2019 7:21:58 PM; Mr. Puorro: I think we have a leak in our India team. Anyway you can find out?

26 5/9/2019 7:24:00 PM; Mr. Williams: Will do

27 5/9/2019 7:24:08 PM; Mr. Williams: Can you get me an offer letter

28 5/9/2019 7:24:14 PM; Mr. Williams: kidding

1 5/9/2019 8:19:42 PM; Mr. Williams: Ok

2 5/9/2019 8:19:45 PM; Mr. Williams: Have info

3 5/9/2019 8:20:09 PM; Mr. Williams: I'm open the rest of the day in 11 mins - call me when it works

4 5/9/2019 9:22:01 PM; Mr. Puorro: Free?

5 5/9/2019 9:22:09 PM; Mr. Williams: yes sir

6 160. On information and belief, Mr. Williams shared Cisco Confidential Materials with Mr.
7 Puorro over the phone on May 9, 2019.

8 161. Throughout Mr. Williams' interview process with Poly, Mr. Williams consulted with
9 an individual, who was formerly a Cisco Senior Vice President whom Poly was interested in hiring as
10 a consultant ("Consultant") for interview coaching and job transition strategies. Mr. Puorro introduced
11 Consultant to Poly, where he was indeed later employed as a consultant. On information and belief,
12 Mr. Puorro used Mr. Williams' relationship with Consultant as means to bring Cisco Confidential
13 Materials to Poly. On information and belief, Consultant began working for Poly part time on or
14 around July 29, 2019.

15 5/22/2019 10:59:19 PM; Mr. Williams: I'm having dinner with [CONSULTANT] tonight

16 5/22/2019 10:59:51 PM; Mr. Williams: Let me know if you want me to pass on anything

17 162. On May 25, 2019, on information and belief, Mr. Williams shared Cisco Confidential
18 Materials with Mr. Puorro. "I have something you probably want to know." Mr. Williams said "Just
19 ring me when you can sneak away - don't want to put this one in writing."

20 163. Mr. Williams had an interview scheduled with a Poly executive on June 12, 2019.

21 164. In preparation for the June 12 interview, Mr. Williams prepared a document containing
22 talking points and a job transition strategy. This document indicated that Mr. Williams intended to
23 share with Poly highly confidential and non-public financial data related to Cisco's collaboration
24 business that is directly competitive with Poly. Specifically, the document included a breakdown of
25 bookings data from Cisco's global collaboration business and the growth rate of Cisco's collaboration
26 business. Moreover, the document provided a geographic breakdown of Cisco's global collaboration
27 business, and identified the growth rate of each geographic constituent. The document also further
28 broke down the largest geographic category by segment and country, and provided corresponding

1 growth rates for each segment/country. The document also explained why Cisco's sales to various
 2 market segments were increasing or decreasing, and the strategies Cisco employed to secure this
 3 growth. The document further described a Cisco sales strategy named "Project Liberator." On June
 4 11, 2019, Mr. Williams emailed this market and strategy data outside of Cisco to Consultant, who Mr.
 5 Williams knew was not authorized by Cisco to have access to Cisco Confidential Materials.

6 165. The market and strategy data that Mr. Williams sent to Consultant is a compilation of
 7 Cisco's confidential financial and business information that is not publicly available, that Cisco has
 8 taken reasonable measures to keep secret, and that derives independent economic value from not being
 9 generally known to, and not being readily ascertainable through proper means by, another person who
 10 can obtain economic value from the disclosure or use of the information.

11 166. On information and belief, Mr. Williams shared Cisco's market and strategy data with
 12 Poly at the June 12 interview. During or immediately after the June 12 interview, Poly invited Mr.
 13 Williams to an additional round of executive interviews in California on June 28, 2019. Mr. Williams
 14 accepted the invitation, and flew to San Francisco, California on June 28, 2019.

15 167. In preparation for the June 28 interviews, Mr. Williams prepared a "discussion guide"
 16 PowerPoint presentation. This presentation contained Mr. Williams' plans for accelerating sales at
 17 Poly, which included Cisco's product strategy and other financial data, with the admonition that "Poly
 18 has to be on Par with Cisco." Mr. Williams later emailed a version of this presentation to Second Poly
 19 Executive at the executive's personal email address as opposed to the executive's Poly email.

20 168. Information concerning Cisco's product strategies and other financial data are forms of
 21 business information that are not publicly available, that Cisco has taken reasonable measures to keep
 22 secret, and that derive independent economic value from not being generally known to, and not being
 23 readily ascertainable through proper means by, another person who can obtain economic value from
 24 the disclosure or use of the information.

25 169. On June 28, 2019, before Mr. Williams was to interview with Poly executives, Mr.
 26 Puorro contacted Mr. Williams to inquire about a potential Limited Restructuring ("LR"), including
 27 layoffs, in Cisco's Collaboration Business Unit ("BU"). Mr. Puorro stated "I heard more LR in the
 28 BU's . . . Wonder if [Cisco Employee] is safe or not." Mr. Puorro asked Mr. Williams to "Dig for

1 me?” On information and belief, Mr. Williams investigated on behalf of Mr. Puorro and provided
 2 details on the magnitude of the potential LR.

3 170. Information concerning Cisco’s potential LR’s is a form of business information that
 4 is not publicly available, that Cisco has taken reasonable measures to keep secret, and that derives
 5 independent economic value from not being generally known to, and not being readily ascertainable
 6 through proper means by, another person who can obtain economic value from the disclosure or use
 7 of the information.

8 171. On July 1, 2019, Mr. Puorro asked Mr. Williams if Cisco had performed the potential
 9 LR yet. Mr. Williams provided a detailed response.

10 172. Between July 1 and August 19, Mr. Williams contacted Mr. Puorro more than 20 times
 11 concerning the potential employment opportunity at Poly. Mr. Puorro provided only terse responses
 12 suggesting that he was too busy to discuss the potential employment opportunity for Mr. Williams at
 13 Poly.

14 173. On July 31, 2019, Mr. Williams sent a message to Second Poly Executive in which Mr.
 15 Williams proposed that it was “[t]ime to execute Project Liberator while Cisco is further distracted,
 16 grow sales and gain marketshare.” Project Liberator is an ongoing Cisco sales strategy that Mr.
 17 Williams was involved with developing and executing while at Cisco. The specific details and tactics
 18 of Project Liberator are Cisco Confidential Materials.

19 174. On August 19, 2019, Mr. Williams told Mr. Puorro about two individuals who had just
 20 left Cisco. Mr. Williams gave Mr. Puorro the names of additional people that Mr. Williams believed
 21 Mr. Puorro could recruit to Poly.

22 175. On August 22, 2019, Mr. Williams sent an email to Second Poly Executive’s personal
 23 gmail account describing his vision for executing “Project x” at Poly. Project x is a Cisco sales strategy
 24 that Mr. Williams was involved with developing and executing while at Cisco. The specific details
 25 and tactics of Project x are Cisco Confidential Materials. Mr. Williams discussed Project x with
 26 Second Poly Executive. The Second Poly Executive asked Mr. Williams to connect with Mr. Puorro
 27 and yet another Poly executive (“Third Poly Executive”) to “figure out next steps to execute the

1 concept” Mr. Williams subsequently shared the details of Project x with Mr. Puorro and Third
 2 Poly Executive.

3 176. On August 27, 2019, Mr. Williams informed Mr. Puorro about Cisco’s investment in
 4 an emerging technology. Mr. Puorro then asked Mr. Williams about an internal Cisco meeting:

5 8/27/2019 6:58:32 PM; Mr. Puorro: How was UC break out yesterday?

6 8/27/2019 7:05:20 PM; Mr. Williams: Just got to my room if you want to chat

7 8/27/2019 7:05:32 PM; Mr. Puorro: Getting on plane..

8 8/27/2019 7:06:09 PM; Mr. Williams: Sounds good - ping me later - don’t want to put anything
 9 on Text that I don’t want Cisco to have!

10 177. Upon information and belief, Mr. Williams later orally provided Cisco Confidential
 11 Materials about the internal Cisco meeting to Mr. Puorro.

12 178. On August 28, 2019, Mr. Williams shared pictures from this internal meeting with Mr.
 13 Puorro. These pictures contained Cisco’s screenshots of presentations and an image of a new Cisco
 14 headset. Mr. Williams communicated to Mr. Puorro that he was “so ready to show [Cisco] that Poly
 15 can inflict pain.” Mr. Williams referred to Cisco’s upcoming products by stating “They’ve got some
 16 good [expletive] coming.” Mr. Puorro asked “[d]oes it work with Zoom.” On information and belief,
 17 Mr. Williams’ response reflected Cisco Confidential Information shared at the internal meeting. Mr.
 18 Williams also provided Mr. Puorro with details from a presentation at this Cisco internal meeting,
 19 explaining Cisco’s competitive focus.

20 179. On September 3, 2019, Mr. Puorro intentionally interfered with Mr. Williams’ duty of
 21 loyalty to Cisco, by inducing Mr. Williams to divert a partnership opportunity from Cisco to Poly.
 22 Mr. Williams informed Mr. Puorro that he was meeting with a Cisco partner named RoomReady (also
 23 known as “Zeller Digital,” or “ZDI”), and said that he was “Looking at them from the Cisco lens. I
 24 could easily change that lens though.” Mr. Williams further stated that he was “[e]xcited to get going
 25 and help [Poly] scale this.” On information and belief, and as substantiated by the subsequent events
 26 detailed below, Mr. Williams and Mr. Puorro agreed that Mr. Williams would pursue the RoomReady
 27 opportunity on Poly’s behalf despite the fact that Mr. Williams was still employed by Cisco.

1 180. Mr. Williams then met with Aaron McArdle, President and CEO of RoomReady on
 2 September 3, 2019. Mr. Williams spent this visit with RoomReady and Mr. McArdle advancing Poly's
 3 interests in a potential partnership, rather than Cisco's interests in its existing partnership. The day of
 4 the meeting with Mr. McArdle, Mr. Williams told Mr. Puorro "*I've been talking about you guys all*
 5 *day* – These room ready guys have some really good stuff" and "*[y]our ears should be burning.*" Mr.
 6 Williams then introduced Mr. McArdle to Consultant (who is now Poly's Chief Revenue Officer) to
 7 facilitate further discussion of a Poly/RoomReady partnership.

8 181. Internally at Cisco, Mr. Williams described his one night trip as a "Partner meeting
 9 with ZDI – Collaboration Partner" and he billed the \$916.19 cost of his hotel, rental car, and flights
 10 and \$875.62 in other expenses to Cisco. Cisco approved these expenses believing Mr. Williams was
 11 using his meetings with RoomReady and Mr. McArdle to advance Cisco's business interests. Instead,
 12 Mr. Williams used the trip to broker a relationship between Poly and RoomReady.

13 182. Through Mr. Williams' connection, Mr. McArdle and Consultant held high level
 14 discussions about market strategy, RoomReady's growth, and Poly. For example, on or around
 15 September 13, 2019, Mr. McArdle and Consultant held a discussion in which they discussed
 16 RoomReady's goals, industry direction, and, on information and belief, partnership opportunities with
 17 Poly. Mr. McArdle and Consultant scheduled an in-person meeting for October 2, 2019 in Normal,
 18 Illinois. Consultant then traveled to Normal for this meeting and, on information and belief, advanced
 19 Poly's business interests in a potential partnership with RoomReady at this meeting

20 183. As part of his PIIA, Mr. Williams agreed to "not provide consulting services to or
 21 become an employee of, any other firm or person engaged in a business in any way competitive with
 22 [Cisco] . . . without first informing [Cisco] . . . and obtaining prior written consent." Mr. Puorro (an
 23 individual formerly subject to the same requirements as a former Cisco employee with his own PIIA)
 24 and Poly intentionally interfered with this contractual relationship by encouraging Mr. Williams to
 25 divert the partnership opportunity with RoomReady from Cisco to Poly.

26 184. Upon information and belief, on September 7, 2019, Mr. Puorro solicited Cisco
 27 Confidential Materials from Mr. Williams. Mr. Puorro and Mr. Williams had a conversation during
 28 which Mr. Williams communicated Cisco Confidential Materials to Mr. Puorro.

1 9/7/2019 2:42:47 PM; Mr. Puorro: I'm curious how is my old [REDACTED] product doing?

2 9/7/2019 2:43:31 PM; Mr. Williams: I asked that very question earlier this week

3 9/7/2019 2:43:41 PM; Mr. Williams: REDACTED

4 9/7/2019 2:44:51 PM; Mr. Puorro: I think [REDACTED] tries to kill it

5 9/7/2019 2:45:07 PM; Mr. Williams: Talk ?

6 9/7/2019 2:46:04 PM; Mr. Williams: Just in case big brother is watching...

7 9/7/2019 2:46:42 PM; Mr. Puorro: Calling

8
9 185. On September 12, 2019, Mr. Williams notified Mr. Puorro that he had turned down a
10 job offer from another company, and that he hoped to hear something from Poly that day. He then
11 revealed details about a prospective Cisco LR, and identified a Cisco employee for Poly to recruit.

12 186. On September 13, 2019, Mr. Williams told Mr. Puorro that he had heard Poly was
13 “having hell with Cisco legal,” apparently a reference to Cisco’s communication with Poly’s General
14 Counsel regarding Dr. Chung and Mr. He. Mr. Puorro stated “we are past that I believe.” Mr. Williams
15 said “They aren’t going to give two [expletive] about me with where I’m at now.” Mr. Williams then
16 told Mr. Puorro that he had “interesting rumors” about Cisco and Collaboration and wished to speak
17 with Mr. Puorro live. Mr. Puorro called Mr. Williams minutes later.

18 187. Also, on September 16, 2019, Mr. Williams communicated with Mr. Puorro and Third
19 Poly Executive about Project x. Mr. Williams conveyed to Second Poly Executive that these were
20 “Great conversations” and asked Second Poly Executive if anything further was required.

21 188. On September 17, Second Poly Executive said that he would get the HR people “in
22 gear today.” Second Poly Executive asked Poly’s human resources department to move fast.

23 189. On September 18, 2019, Mr. Williams notified Mr. Puorro of a prospective LR at Cisco.
24 Mr. Williams also provided details concerning the status of a Cisco business unit, and identified an
25 employee potentially impacted by the LR who he believed could be recruited by Poly.

26 190. On information and belief, on September 19, 2019, Mr. Williams was informed an
27 employment offer at Poly would be forthcoming.

28 191. Mr. Williams received a formal employment offer to join Poly on September 26, 2019.

1 192. Information concerning Cisco's investments in emerging technologies, Cisco's
 2 competitive focus, Cisco's sales opportunities and customer lists, Cisco's new products, and Cisco's
 3 future plans for its current products are forms of business information that are not publicly available,
 4 that Cisco has taken reasonable measures to keep secret, and that derives independent economic value
 5 from not being generally known to, and not being readily ascertainable through proper means by,
 6 another person who can obtain economic value from the disclosure or use of the information.

7 193. On October 10, 2019, Mr. Williams received his Poly network credentials.

8 194. On October 11, 2019, Mr. Williams received from Poly his first week schedule, with a
 9 planned start date of October 14, 2019.

10 195. On October 12, 2019, Mr. Williams signed a Poly form certifying that he had not
 11 downloaded onto any device any of Cisco's confidential information. Mr. Williams also certified that
 12 Cisco had reviewed and/or deleted, or that he had deleted, any of Cisco's confidential information.
 13 Mr. Williams also certified that he had returned all of Cisco's equipment and property to Cisco.

14 196. Mr. Williams October 12, 2019 certification was false. On information and belief, Poly
 15 knew, or was willfully blind to the fact, that Mr. Williams was still employed at Cisco at the time of
 16 the certification and had access to and possession of Cisco Confidential Materials and equipment. For
 17 example, Mr. Williams indicated to Poly's human resources department that he would like to begin
 18 regular work activities on October 15, because of issues with Cisco's human resources department.

19 197. Mr. Williams traveled to Santa Clara, California on October 13, 2019.

20 198. After receiving and accepting Poly's offer of employment, Mr. Williams requested a
 21 monetary separation package from Cisco. Even though he was directly asked during these discussions
 22 about his plans after leaving Cisco, Mr. Williams claimed that he was going to work at his church and
 23 focus on personal issues. In light of these circumstances and to help Mr. Williams with his family,
 24 Cisco offered Mr. Williams two months sales pay, in addition to a lump sum payment to cover two
 25 months COBRA health care premiums. At the time, Mr. Williams of course already had accepted an
 26 offer with Poly, which included health benefits.

27 199. Mr. Williams returned his laptop to Cisco's San Jose office in person. Mr. Williams
 28 was obligated by Cisco to return all other Cisco Confidential Materials he possessed at that time.

1 200. Mr. Williams' employment with Cisco terminated on October 15, 2019.

2 201. Mr. Williams' disclosures of Cisco Confidential Information to Mr. Puorro were
3 outside the scope of his employment at Cisco.

4 202. During the course of his employment at Cisco, Mr. Williams ran a home server that he
5 used to store a Time Machine backup of his Cisco laptop. This backup contained, and, on information
6 and belief, still contains Cisco Confidential Materials, including detailed information about Cisco's
7 sales forecasts and opportunities, including customer names, commitments, and upsides. Mr. Williams
8 did not return this backup to Cisco upon his termination. Mr. Williams' retention of this backup was
9 outside the scope of his employment at Cisco.

10 **D. Poly**

11 203. Paragraphs 1 through 187 are incorporated by reference as if fully stated herein.

12 204. Poly acquired and used Cisco's trade secrets through the actions of its employee, Dr.
13 Chung. For example, Dr. Chung accessed Cisco Confidential Materials that he misappropriated at
14 least on February 26, March 8, and March 24, 2019 while he was employed at Poly. On information
15 and belief, Dr. Chung used these Cisco Confidential Materials within the course and scope of his
16 employment at Poly. The Cisco Confidential Materials accessed by Dr. Chung while he was employed
17 at Poly contain Cisco's trade secrets.

18 205. On September 9, 2019, Cisco notified Poly through its General Counsel that Dr. Chung
19 had misappropriated Cisco Confidential Materials. Poly did not place Dr. Chung on administrative
20 leave at this time, and, on information and belief, took no action adverse to Dr. Chung. Having not
21 heard back from Poly, Cisco followed up on September 17, 2019, to reiterate its concerns about Dr.
22 Chung. Poly's General Counsel stated that Dr. Chung denied taking any of Cisco Confidential
23 Materials. On September 26, 2019, Poly wrote to Cisco and provided follow up information which
24 confirmed that Dr. Chung's representations to Poly were false. Indeed, Dr. Chung had, in fact, taken
25 Cisco Confidential Materials to Poly, including at least the EA Document and Webex Vision
26 Document. Despite his dishonesty, Poly still took no action adverse to Dr. Chung. On October 9,
27 2019, Cisco again contacted Poly about its concerns with Dr. Chung, and also provided Poly with
28 information confirming that Dr. Chung's explanation for the whereabouts of the First Seagate Drive

1 and Second Seagate Drive was not credible. Only then did Poly place Dr. Chung on a brief
 2 administrative leave. Cisco and Poly then arranged for Dr. Chung's devices to be analyzed by a third
 3 party. Dr. Chung did not turn over the First Seagate Drive or the Second Seagate Drive for analysis.
 4 The forensic investigation revealed that Dr. Chung accessed Cisco Confidential Materials after the
 5 start of his employment with Poly, that he emailed Cisco Confidential Materials to his Poly email
 6 address, and that apparent data wiping procedures were performed on at least the Sandisk and Samsung
 7 Drives after Cisco requested Dr. Chung to preserve all data. The third party forensics lab reported
 8 these results to Poly. The whereabouts of the First Seagate Drive and Second Seagate Drive, which
 9 contain Cisco Confidential Materials, remain unknown to Cisco, and, on information and belief, to
 10 Poly. Nevertheless, on the evening of November 13, Poly informed Cisco that it inexplicably intended
 11 to return Dr. Chung to his position the very next day.

12 206. On October 18, 2019, when the severity and gravity of Dr. Chung and Mr. He's
 13 misappropriation became clear to Poly, Poly's General Counsel raised allegations (later proved to be
 14 unsupported) that a former Poly employee who had recently joined Cisco exfiltrated confidential Poly
 15 materials on a thumb drive. On information and belief, Poly raised these allegations as a tactical
 16 maneuver to compel Cisco to cease its investigations into Dr. Chung and Mr. He. Cisco immediately
 17 placed this employee on administrative leave and performed a thorough investigation. Cisco's
 18 investigation revealed that Poly's claims had no merit. When Cisco revealed the results of its
 19 investigation, Poly did not challenge the results. Rather, Poly raised an additional allegation against
 20 this same employee that Cisco investigated and found was not credible.

21 207. Poly knew or should have known that Dr. Chung still possessed, and intended to use in
 22 his employment at Poly, Cisco Confidential Materials when it permitted him to return to work on
 23 November 14, 2019.

24 208. Poly ratified Dr. Chung's misappropriation of Cisco's trade secrets by failing to
 25 terminate his employment after discovering that he had, in fact, misappropriated Cisco Confidential
 26 Materials.

209. Poly also ratified Dr. Chung's misappropriation of Cisco's trade secrets by permitting him to return to work when it knew or should have known that Dr. Chung still possessed Cisco Confidential Materials.

210. Poly also acquired and used Cisco's trade secrets through the actions of its former employee, James He. For example, Mr. He accessed Cisco Confidential Materials that he misappropriated on June 27, July 1, and July 15, 2019 while he was employed at Poly. On information and belief, Mr. He used these Cisco Confidential Materials within the course and scope of his employment at Poly. The Cisco Confidential Materials accessed by Mr. He while he was employed at Poly contain Cisco's trade secrets.

211. Poly also acquired through improper means, and on information and belief, used Cisco's trade secrets through the actions of its officer, Mr. Puorro. Mr. Puorro acted in concert with Mr. Williams to acquire and use Cisco Confidential Materials at Poly. On information and belief, Poly's executives were aware of Mr. Puorro's conduct, and acquiesced to it. Poly's executives, including at least Second Poly Executive and Third Poly Executive knew or should have known that Mr. Williams was revealing Cisco Confidential Materials to Mr. Puorro, at least because Mr. Williams shared details relating to Project x, including that it was a Cisco project, to the Second Poly Executive and Third Poly Executive. Furthermore, Mr. Puorro's inducement of Mr. Williams to disclose Cisco trade secrets to him and others at Poly was within the course and scope of Mr. Puorro's employment at Poly and was intended to benefit Poly to the detriment of Cisco.

COUNT I

Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Dr. Chung

212. Paragraphs 1 through 211 are incorporated by reference as if fully stated herein.

213. Dr. Chung's misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

214. Cisco Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco technical information such as source code, schematics, design details and specifications, user feedback, design documentation, and features relating to Cisco's

1 existing and future products, as well as Cisco business information such as marketing strategy, cost
 2 and pricing information, and payment information.

3 215. Dr. Chung misappropriated Cisco's trade secrets by improper means (including, for
 4 example, by systematically transferring Cisco Confidential Materials out of Cisco immediately
 5 preceding his departure), by disclosure without authorization (including, for example, by uploading
 6 Cisco Confidential Materials to Poly's Sharepoint site), and by use without authorization (including,
 7 for example, to obtain a competitive advantage in his product development efforts).

8 216. Dr. Chung has maintained and continues to maintain in his possession the wrongfully
 9 acquired Cisco documents and materials after the termination of his employment with Cisco.

10 217. Dr. Chung used and continues to use Cisco trade secret contained in these wrongfully
 11 acquired Cisco documents by way of providing these documents to Poly and/or accessing these
 12 documents.

13 218. Dr. Chung's possession after leaving Cisco, acquisition, disclosure, and/or use of Cisco
 14 trade secrets was and is without Cisco's express or implied consent.

15 219. Cisco trade secrets were developed over time after expenditure of significant effort and
 16 resources.

17 220. Cisco trade secrets are not publicly available, and are kept within the knowledge and
 18 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
 19 bound by contractual obligations of confidentiality.

20 221. Cisco has taken reasonable measures to keep its trade secret information secret.

21 222. Cisco communicates the importance of maintaining confidentiality to its employees in
 22 various means and forms, including but not limited to the Proprietary Information and Inventions
 23 Agreements and termination letters.

24 223. On February 9, 2007, Dr. Chung executed the Chung PIIA in consideration for his
 25 employment with Cisco.

26 224. The Chung PIIA protects Cisco's proprietary information, which was defined in the
 27 Chung PIIA as (i) information that was or will be developed, created, or discovered by or on behalf of
 28 Cisco, or which became or will become known by, or was or is conveyed to Cisco, which has

1 commercial value in Cisco's business, or (ii) any other information that Cisco does not want publicly
 2 disclosed. The Chung PIIA further states that Cisco proprietary information includes but is not limited
 3 to software programs and subroutines, source and object code, algorithms, trade secrets, designs,
 4 technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or not),
 5 works of authorship, formula, business and product development plans, customer lists, terms of
 6 compensation and performance levels of Cisco employees, and other information concerning Cisco's
 7 actual or anticipated business, research or development, or which is received in confidence by or for
 8 Cisco from any other source, or any document that is marked as "confidential."

9 225. By signing the Chung PIIA, Dr. Chung agreed that he would "not remove any Company
 10 Documents and Materials from the business premises of Cisco or deliver any Company Documents
 11 and Materials to any person or entity outside of Cisco, except as [] required to do in connection with
 12 performing the duties of [his] employment." Dr. Chung also agreed that "immediately upon the
 13 termination of [his] employment," he would "return all Company Documents and Materials, apparatus,
 14 equipment and other physical property, or any reproductions of such property"

15 226. Dr. Chung took intentional and systematic steps during at least a three and a half week
 16 period before the termination of his employment to transfer thousands of documents containing Cisco
 17 Confidential Materials out of Cisco.

18 227. Upon termination of Dr. Chung's employment at Cisco on February 18, 2019, Cisco
 19 delivered to Dr. Chung a termination letter, reminding Dr. Chung of his continuing obligations to
 20 Cisco, including the duty to maintain confidentiality of Cisco confidential information, the duty of
 21 non-solicitation within one year after the termination of Dr. Chung's employment, and the duty to
 22 return any Cisco documents as soon as possible.

23 228. Dr. Chung did not return the Cisco Confidential Materials that he had systematically
 24 transferred out of Cisco.

25 229. Cisco implements security measures such as electronic access points to restrict access
 26 to Cisco's confidential and proprietary information.

27

28

230. Cisco trade secrets derive independent economic value, actual or potential, from not being generally known to, and/or not being readily ascertainable through proper means by, the public or other persons who can obtain economic value from the disclosure or use of the information.

231. Cisco's trade secrets at issue in this case are related to products that are placed in or are intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. § 1836.

232. Defendant Dr. Chung's misappropriation of Cisco's trade secret information was willful and malicious.

¹⁰ 233. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

11 234. On information and belief, if Defendant Dr. Chung's conduct is not enjoined,
12 Defendant will continue to misappropriate, disclose, and use for his own benefit and to Cisco's
13 detriment Cisco's trade secret information.

14 235. Because Cisco's remedy at law is inadequate, Cisco seeks preliminary and permanent
15 injunctive relief to recover and protect its confidential, proprietary, and trade secret information and
16 other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage
17 that otherwise would be derived from Defendant Dr. Chung's continued misappropriation of Cisco's
18 trade secret information.

COUNT II

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Dr. Chung

21 236. Paragraphs 1 through 235 are incorporated by reference as if fully stated herein.

22 237. Dr. Chung’s misappropriation of trade secrets is independently actionable under
23 California’s Uniform Trade Secrets Act (“CUTSA”), Cal. Civ. Code § 3426 et seq.

24 ||| 238. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

25 239. Defendant's misappropriation of Cisco's trade secret information was willful and
26 malicious.

240. On information and belief, if Dr. Chung is not enjoined, the Defendant will continue to misappropriate, disclose, and use for his own benefit and the benefit of others and to Cisco's detriment Cisco's trade secret information.

241. Because Cisco's remedy at law is inadequate, Cisco seeks preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code §3426.2.

COUNT III

Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Mr. He

242. Paragraphs 1 through 241 are incorporated by reference as if fully stated herein.

243. Mr. He's misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

244. Cisco Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco technical information such as design and architectural documents, hardware diagrams, schematics, source code stacks, and engineering specification relating to existing and future Cisco products, as well as business information such as relating to marketing plans, business opportunities, and revenue and cost information that is not disclosed in publicly available financial reports.

245. Mr. He's misappropriated Cisco's trade secrets by improper means (including, for example, by systematically transferring Cisco Confidential Materials out of Cisco immediately preceding his departure), on information and belief by disclosure without authorization, and by use without authorization (including, for example, to obtain a competitive advantage in his product development efforts).

246. Mr. He maintained in his possession these wrongfully acquired Cisco documents and materials after the termination of his employment with Cisco.

1 247. On information and belief, Mr. He has used Cisco trade secrets contained in these
2 wrongfully acquired Cisco documents.

3 248. Mr. He's possession after leaving Cisco, acquisition, disclosure, and/or use of Cisco
4 trade secrets was and is without Cisco's express or implied consent.

5 249. Cisco trade secrets were developed over time after expenditure of significant effort and
6 resources.

7 250. Cisco trade secrets are not publicly available, and are kept within the knowledge and
8 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
9 bound by contractual obligations of confidentiality.

10 251. Cisco has taken reasonable measures to keep its trade secret information secret.

11 252. Cisco communicates the importance of maintaining confidentiality to its employees in
12 various means and forms, including but not limited to the Proprietary Information and Inventions
13 Agreements and termination letters.

14 253. On March 8, 1999, Mr. He executed the He PIIA in consideration for his employment
15 with Cisco.

16 254. The He PIIA protects Cisco's proprietary information, which was defined in the He
17 PIIA as information that was developed, created, or discovered by or on behalf of Cisco, or which
18 became or will become known by, or was or is conveyed to Cisco, which has commercial value in
19 Cisco's business. The He PIIA further states that Cisco proprietary information includes but is not
20 limited to software programs and subroutines, source and object code, algorithms, trade secrets,
21 designs, technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or
22 not), works of authorship, formula, business and product development plans, customer lists, terms of
23 compensation and performance levels of Cisco employees, and other information concerning Cisco's
24 actual or anticipated business, research or development, or which is received in confidence by or for
25 Cisco from any other person.

26 255. By signing the He PIIA, Mr. He agreed that he would "not remove any Company
27 Documents and Materials from the business premises of [Cisco] or deliver any Company Documents
28 and Materials to any person or entity outside [Cisco], except as [] required to do in connection with

1 performing the duties of [his] employment.” Mr. He also agreed that “immediately upon the
 2 termination of [his] employment,” he would “return all Company Documents and Materials, apparatus,
 3 equipment and other physical property, or any reproductions of such property”

4 256. Mr. He took intentional and systematic steps at least during a six week period before
 5 the termination of his employment to transfer thousands of documents containing Cisco Confidential
 6 Materials out of Cisco.

7 257. Cisco implements security measures such as electronic access points to restrict access
 8 to Cisco’s confidential and proprietary information.

9 258. Cisco trade secrets derive independent economic value, actual or potential, from not
 10 being generally known to, and/or not being readily ascertainable through proper means by, the public
 11 or other persons who can obtain economic value from the disclosure or use of the information.

12 259. Cisco’s trade secrets at issue in this case are related to products that are placed in or are
 13 intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products
 14 around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. §
 15 1836.

16 260. Defendant Mr. He’s misappropriation of Cisco’s trade secret information was willful
 17 and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. § 1836(b)(3)(C)
 18 and its attorneys’ fees and costs under 18 U.S.C. § 1836(b)(3)(D).

19 261. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

20 262. On information and belief, if Defendant Mr. He’s conduct is not remedied and/or
 21 enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to
 22 Cisco’s detriment Cisco’s trade secret information.

23 263. Because Cisco’s remedy at law is inadequate, Cisco seeks, in addition to damages,
 24 preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and
 25 trade secret information and other legitimate business interests. Injunctive relief is necessary to
 26 eliminate the commercial advantage that otherwise would be derived from Mr. He’s continued
 27 misappropriation of Cisco’s trade secret information.

28

COUNT IV**Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Mr. He**

264. Paragraphs 1 through 263 are incorporated by reference as if fully stated herein.

265. Mr. He's misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 et seq.

266. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

267. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

268. Defendant's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

269. On information and belief, if the Defendant's conduct is not remedied, and if the Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for their own benefit and to Cisco's detriment Cisco's trade secret information.

270. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code §3426.2.

COUNT V¹**Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Mr. Williams**

271. Paragraphs 1 through 270 are incorporated by reference as if fully stated herein.

272. Mr. Williams' misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

28 ¹ Count V against Mr. Williams is stayed pending arbitration. See Dkt. 97 at 20.

1 273. Cisco Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For
 2 example, these trade secrets include Cisco's market and strategy data, partner margins, potential
 3 limited restructurings, information concerning Cisco's emerging technologies, competitive focus,
 4 sales opportunities and customer lists, product pipelines, and future plans for current products. On
 5 information and belief, the Cisco documents stored on Mr. Williams' server backup include Cisco's
 6 trade secrets such as customer lists, pricing information and strategic business development plans.

7 274. Mr. Williams misappropriated Cisco's trade secrets by acquisition by improper means
 8 (including, for example, by retaining possession of Cisco Confidential Materials after the termination
 9 of his employment), by disclosure without authorization (including, for example, by disclosing Cisco
 10 Confidential Materials to Mr. Puorro, to other Poly executives, and to Consultant), and by use without
 11 authorization (such as to obtain a competitive business advantage in sales and marketing).

12 275. Mr. Williams' possession after leaving Cisco, acquisition, disclosure, and/or use of
 13 Cisco trade secrets was and is without Cisco's express or implied consent.

14 276. Cisco trade secrets were developed over time after expenditure of significant effort and
 15 resources.

16 277. Cisco trade secrets are not publicly available, and are kept within the knowledge and
 17 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
 18 bound by contractual obligations of confidentiality.

19 278. Cisco has taken reasonable measures to keep its trade secret information secret.

20 279. Cisco communicates the importance of maintaining confidentiality to its employees in
 21 various means and forms, including but not limited to the Proprietary Information and Inventions
 22 Agreements and termination letters.

23 280. On July 20, 1998, Mr. Williams executed the Williams PIIA in consideration for his
 24 employment with Cisco.

25 281. The Williams PIIA protects Cisco's proprietary information, which was defined in the
 26 Williams PIIA as information that was developed, created, or discovered by or on behalf of Cisco, or
 27 which became or will become known by, or was or is conveyed to Cisco, which has commercial value
 28 in Cisco's business. The Williams PIIA further states that Cisco proprietary information includes but

1 is not limited to software programs and subroutines, source and object code, algorithms, trade secrets,
2 designs, technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or
3 not), works of authorship, formula, business and product development plans, customer lists, terms of
4 compensation and performance levels of Cisco employees, and other information concerning Cisco's
5 actual or anticipated business, research or development, or which is received in confidence by or for
6 Cisco from any other person.

7 282. By signing the Williams PIIA, Mr. Williams agreed that he would "keep in confidence
8 and trust and will not use or disclose any Proprietary Information of anything relating to it without the
9 prior written consent of an officer of the company, except as may be necessary in the ordinary course
10 of performing my duties to the Company." Mr. Williams also agreed that he would "not remove any
11 Company Documents and Materials from the business premises of [Cisco] or deliver any Company
12 Documents and Materials to any person or entity outside [Cisco], except as [] required to do in
13 connection with performing the duties of [his] employment." Mr. Williams also agreed that
14 "immediately upon the termination of [his] employment," he would "return all Company Documents
15 and Materials, apparatus, equipment and other physical property, or any reproductions of such
16 property"

17 283. Before leaving Cisco, Mr. Williams took intentional steps to transfer Cisco
18 Confidential Materials out of Cisco.

19 284. Cisco implements security measures such as electronic access points to restrict access
20 to Cisco's confidential and proprietary information.

21 285. Cisco trade secrets derive independent economic value, actual or potential, from not
22 being generally known to, and/or not being readily ascertainable through proper means by, the public
23 or other persons who can obtain economic value from the disclosure or use of the information.

24 286. Cisco's trade secrets at issue in this case are related to products that are placed in or are
25 intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products
26 around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. §
27 1836.

28

287. Defendant Mr. Williams' misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. § 1836(b)(3)(C) and its attorneys' fees and costs under 18 U.S.C. § 1836(b)(3)(D).

^{288.} Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

289. On information and belief, if Defendant Mr. Williams' conduct is not remedied and /or enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to Cisco's detriment Cisco's trade secret information.

290. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Mr. Williams' continued misappropriation of Cisco's trade secret information.

COUNT VI²

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Mr. Williams

291. Paragraphs 1 through 290 are incorporated by reference as if fully stated herein.

292. Mr. Williams' misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 *et seq.*

293. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

294. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

295. Defendant's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

² Count VI against Mr. Williams is stayed pending arbitration. See Dkt. 97 at 20.

296. On information and belief, if the Defendant's conduct is not remedied, and if the Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for their own benefit and to Cisco's detriment Cisco's trade secret information.

297. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code §3426.2.

COUNT VII

Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Mr. Puorro

298. Paragraphs 1 through 297 are incorporated by reference as if fully stated herein.

299. Mr. Puorro's misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

300. The materials and information that Mr. Puorro solicited from Mr. Williams contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco's market and strategy data, partner margins, potential limited restructurings, information concerning Cisco's emerging technologies, competitive focus, sales opportunities and customer lists, product pipelines, and future plans for current products.

301. Mr. Puorro misappropriated Cisco's trade secrets by acquisition by improper means (including, for example, by inducing Mr. Williams to reveal Cisco Confidential Materials), by disclosure without authorization (including, for example, by revealing Cisco Confidential Materials to others at Poly), and by use without authorization (such as to obtain a competitive business advantage in sales, marketing, and product development efforts).

302. As a former Cisco employee, Mr. Puorro knew or should have known that Mr. Williams had a duty to maintain secrecy over the materials he induced Mr. Williams to reveal.

303. Mr. Puorro's acquisition, disclosure, and/or use of Cisco trade secrets was and is without Cisco's express or implied consent.

1 304. Cisco trade secrets were developed over time after expenditure of significant effort and
 2 resources.

3 305. Cisco trade secrets are not publicly available, and are kept within the knowledge and
 4 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
 5 bound by contractual obligations of confidentiality.

6 306. Cisco has taken reasonable measures to keep its trade secret information secret.

7 307. Cisco communicates the importance of maintaining confidentiality to its employees in
 8 various means and forms, including but not limited to the Proprietary Information and Inventions
 9 Agreements and termination letters.

10 308. Cisco implements security measures such as electronic access points to restrict access
 11 to Cisco's confidential and proprietary information.

12 309. Cisco trade secrets derive independent economic value, actual or potential, from not
 13 being generally known to, and/or not being readily ascertainable through proper means by, the public
 14 or other persons who can obtain economic value from the disclosure or use of the information.

15 310. Cisco's trade secrets at issue in this case are related to products that are placed in or are
 16 intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products
 17 around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. §
 18 1836.

19 311. Defendant Mr. Puorro's misappropriation of Cisco's trade secret information was
 20 willful and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. §
 21 1836(b)(3)(C) and its attorneys' fees and costs under 18 U.S.C. § 1836(b)(3)(D).

22 312. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

23 313. On information and belief, if Defendant Mr. Puorro's conduct is not remedied and /or
 24 enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to
 25 Cisco's detriment Cisco's trade secret information.

26 314. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages,
 27 preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and
 28 trade secret information and other legitimate business interests. Injunctive relief is necessary to

1 eliminate the commercial advantage that otherwise would be derived from Mr. Williams' continued
 2 misappropriation of Cisco's trade secret information.

3 **COUNT VIII**

4 **Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Mr. Puorro**

5 315. Paragraphs 1 through 314 are incorporated by reference as if fully stated herein.

6 316. Mr. Puorro's misappropriation of trade secrets is independently actionable under
 7 California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 *et seq.*

8 317. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

9 318. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or
 10 reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

11 319. Defendant's misappropriation of Cisco's trade secret information was willful and
 12 malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and
 13 its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

14 320. On information and belief, if the Defendant's conduct is not remedied, and if the
 15 Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for their
 16 own benefit and to Cisco's detriment Cisco's trade secret information.

17 321. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages,
 18 preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and
 19 trade secret information and other legitimate business interests. Injunctive relief is necessary to
 20 eliminate the commercial advantage that otherwise would be derived from Defendant's continued
 21 misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal.
 22 Civ. Code §3426.2.

23 **COUNT IX**

24 **Intentional Interference with a Contractual Relationship by Mr. Puorro**

25 322. Paragraphs 1 through 321 are incorporated by reference as if fully stated herein.

26 323. The Williams PIIA was a written contract between Cisco and Mr. Williams which
 27 prohibited Mr. Williams from using or disclosing any of Cisco's proprietary information, including
 28 trade secrets, without the prior written consent of an officer of the Company.

1 324. Mr. Puorro was aware of the Williams PIIA. For example, Mr. Puorro himself signed
 2 a Proprietary Information And Invention Agreement (The “Puorro PIIA”) which similarly prohibited
 3 the use and disclosure of Cisco’s proprietary information, including trade secrets. Mr. Puorro was
 4 also reminded of his obligations under the PIIA as recently as February 2019. As another example,
 5 Cisco’s practice of entering Proprietary Information and Inventions Agreements with its employees is
 6 well known in the industry generally. As another example, Cisco sent Dr. Chung and Mr. He’s PIIA
 7 agreements to Poly during the course of those investigations, and, on information and belief, those
 8 letters were shared with Mr. Puorro.

9 325. Mr. Puorro engaged in conduct that prevented and/or hindered performance of the
 10 Williams PIIA, for example, by inducing Mr. Williams to reveal Cisco’s proprietary information and
 11 trade secrets to Mr. Puorro and other Poly executives, and by inducing Mr. Williams to breach his
 12 duty of loyalty to Cisco. As another example, Mr. Puorro induced Mr. Williams to advance Poly’s
 13 interests in a partnership with RoomReady, to the detriment of Cisco’s interest in that Partnership,
 14 while Mr. Williams was still a Cisco employee.

15 326. Mr. Puorro intended for Mr. Williams to reveal Cisco’s proprietary information and
 16 trade secrets or knew it was likely. For example, Mr. Williams repeatedly conveyed his desire for a
 17 job at Poly to Mr. Puorro, and Mr. Puorro offered his advocacy in exchange for Mr. Williams’
 18 revealing Cisco Confidential Materials. Moreover, Mr. Puorro continued this course of conduct after
 19 Mr. Williams first revealed Cisco Confidential Materials, and therefore intended for Mr. Williams’
 20 conduct to continue.

21 327. Cisco has been substantially harmed as a proximate result of Mr. Puorro’s conduct. For
 22 example, Mr. Puorro’s intentional interference with the Williams PIIA threatens to damage the value
 23 of Cisco’s trade secret technology and business processes, and has provided Poly with proprietary
 24 information about Cisco’s financial performance, customers, internal business processes, and product
 25 development plans, which, on information and belief, Poly is using for its own benefit and to the
 26 detriment of Cisco.

27 328. Mr. Puorro’s actions were willful, intentional, and malicious. Cisco is therefore
 28 entitled to punitive and exemplary damages.

COUNT X**Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Poly**

329. Paragraphs 1 through 328 are incorporated by reference as if fully stated herein.

330. Poly's misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

331. The materials and information that Mr. Puorro solicited from Mr. Williams contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco's market and strategy data, partner margins, potential limited restructurings, information concerning Cisco's emerging technologies, competitive focus, sales opportunities and customer lists, product pipelines, and future plans for current products. The materials used by Dr. Chung and Mr. He while employed at Poly also included trade secrets, including, for example, non-public design specifications for current and unreleased Cisco products.

332. Poly is vicariously liable for the actions of its officer, Mr. Puorro during the course and scope of his employment at Poly. Mr. Puorro misappropriated Cisco's trade secrets by acquisition by improper means (including, for example, by inducing Mr. Williams to reveal Cisco Confidential Materials), by disclosure without authorization (including, for example, by revealing Cisco Confidential Materials to others at Poly), and by use without authorization (such as to obtain a competitive business advantage in sales, marketing, and product development efforts).

333. Additional Poly officers were aware of Mr. Puorro's inducement of Mr. Williams, and ratified his conduct on behalf of Poly. For example, at least one other Poly officer was aware of Mr. Puorro's inducement of Mr. Williams to disclose Cisco Confidential Material to others at Poly. That other Poly officer further ratified Mr. Puorro's conduct on behalf of Poly by requesting that Mr. Williams disclose Cisco Confidential Material to Poly and others at Poly.

334. Poly is vicariously liable for the actions of Dr. Chung and Mr. He during the course and scope of their employment at Poly. Dr. Chung misappropriated Cisco's trade secrets by improper means (including, for example, by systematically transferring Cisco Confidential Materials out of Cisco immediately preceding his departure), by disclosure without authorization (including, for example, by uploading Cisco Confidential Materials to Poly's Sharepoint site), and by use without

1 authorization (including, for example, to obtain a competitive advantage in his product development
 2 efforts). Dr. Chung further operated within the scope of his employment with Poly when he recruited
 3 Mr. He to join Poly. Mr. He's misappropriated Cisco's trade secrets by improper means (including,
 4 for example, by systematically transferring Cisco Confidential Materials out of Cisco immediately
 5 preceding his departure), on information and belief by disclosure without authorization, and by use
 6 without authorization (including, for example, to obtain a competitive advantage in his product
 7 development efforts).

8 335. Poly is further liable for Dr. Chung's acts of misappropriation because it ratified Dr.
 9 Chung's actions and misappropriation of Cisco's trade secrets when it failed to disavow Dr. Chung's
 10 conduct or terminate his employment after Poly had reason to know of Dr. Chung's misappropriation.

11 336. Poly is further liable for Mr. Williams' acts of misappropriation because it ratified Mr.
 12 Williams' actions and misappropriation of Cisco's trade secrets when it hired him after Poly had
 13 reason to know of Mr. Williams' misappropriation through the actions of its senior executives
 14 including Mr. Puorro.

15 337. Upon information and belief, the Poly Executive Officers' familiar with the misconduct
 16 of Mr. Puorro and Mr. Williams were also aware of Poly's decisions with respect to Dr. Chung, thus
 17 demonstrating an intentional and willful disregard for Cisco's trade secrets by Poly.

18 338. Poly's acquisition, disclosure, and/or use of Cisco trade secrets was and is without
 19 Cisco's express or implied consent.

20 339. Cisco trade secrets were developed over time after expenditure of significant effort and
 21 resources.

22 340. Cisco trade secrets are not publicly available, and are kept within the knowledge and
 23 know-how of Cisco employees under strict confidentiality obligations, and only shared with parties
 24 bound by contractual obligations of confidentiality.

25 341. Cisco has taken reasonable measures to keep its trade secret information secret.

26 342. Cisco communicates the importance of maintaining confidentiality to its employees in
 27 various means and forms, including but not limited to the Proprietary Information and Inventions
 28 Agreements and termination letters.

343. Cisco implements security measures such as electronic access points to restrict access to Cisco's confidential and proprietary information.

344. Cisco trade secrets derive independent economic value, actual or potential, from not being generally known to, and/or not being readily ascertainable through proper means by, the public or other persons who can obtain economic value from the disclosure or use of the information.

345. Cisco's trade secrets at issue in this case are related to products that are placed in or are intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. § 1836.

346. Defendant Poly's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. § 1836(b)(3)(C) and its attorneys' fees and costs under 18 U.S.C. § 1836(b)(3)(D).

^{347.} Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

348. On information and belief, if Defendant Poly's conduct is not remedied and/or enjoined, Defendant will continue to misappropriate, disclose, and use for its own benefit and to Cisco's detriment Cisco's trade secret information.

349. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Poly's continued misappropriation of Cisco's trade secret information.

COUNT XI

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Poly

350. Paragraphs 1 through 349 are incorporated by reference as if fully stated herein.

351. Poly's misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 *et seq.*

352. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

353. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

354. Defendant's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

355. On information and belief, if the Defendant's conduct is not remedied, and if the Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for its own benefit and to Cisco's detriment Cisco's trade secret information.

356. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code §3426.2.

COUNT XII

Intentional Interference with a Contractual Relationship by Poly

357. Paragraphs 1 through 356 are incorporated by reference as if fully stated herein

358. Poly is vicariously liable for the actions of its officer, Mr. Puorro, during the course and scope of his employment at Poly. Mr. Puorro was aware of the Williams PIIA, and, within the course and scope of his employment at Poly, engaged in conduct that prevented or hindered performance of that contract, and intended that result. Mr. Puorro's actions proximately caused Cisco substantial harm.

359. Mr. Puorro's actions, which are attributable to Poly, were willful, intentional, and malicious. Cisco is therefore entitled to punitive and exemplary damages.

Prayer For Relief

WHEREFORE, CISCO prays for judgment as follows:

A. Impose preliminary and permanent injunction against Defendants;

B. Award compensatory damages against Messrs. He, Williams, Puorro, and Poly according to the proof;

- C. Award punitive and exemplary damages to deter similar wrongdoings;
- D. Award prejudgment interest at the maximum legal rate as allowed by the law;
- E. Award reasonable attorney's fees;
- F. Award costs of suit herein incurred; and
- G. Such other and further relief as this Court deems just and proper.

Demand For Jury Trial

Plaintiff Cisco hereby demands a trial by jury on all issues so triable.

Dated: June 12, 2020

By: /s/ *Carson Olscheski*

John M. Desmarais (SBN 320875)
DESMARAIS LLP
101 California Street
San Francisco, CA 94111
(415) 573-1900

Justin P.D. Wilcox (admitted pro hac vice)
jwilcox@desmaraisllp.com
Tamir Packin (SBN 317249)
tpackin@desmaraisllp.com
Steven M. Balcof (admitted pro hac vice)
sbalcof@desmaraisllp.com
Carson Olsheski (admitted pro hac vice)
colsheski@desmaraisllp.com
David A. Frey (admitted pro hac vice)
dfrey@desmaraisllp.com
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
(212) 351-3400

Attorneys for Plaintiffs